Contract #: AR3110

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

WellSky Corporation (formerly Mediware Human and Social Services)
Name

11711 West 79th Street
Street Address

Lenexa	KS	66214
City	*State*	*Zip*

Vendor # VC205653 Commodity Code #: 920-05 Legal Status of Contractor: For-Profit Corporation

Contact *Name:* Barry Beus *Phone Number:* 571-234-6642 *Email:* barry.beus@mediware.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Friday, August 09, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

Stephen Greenberg
Stephen Greenberg (Aug 8, 2019)

Aug 8, 2019

Contractor's signature | Date

Stephen Greenberg sg

Type or Print Name and Title

DIVISION OF PURCHASING

Aug 8, 2019

Director, Division of Purchasing | Date

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by receiving party or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any of disclosing party's records, (2) personnel records, (3) information concerning individuals, (4) the Documentation, (5) the design and architecture of the database, and (6) any source and object code of the system is confidential information of disclosing party.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the Master Agreement.

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

Data means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited

control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign its rights, duties or obligations under this Agreement without the prior written consent of the Lead State and such consent shall not be unreasonably withheld. Notwithstanding the foregoing, Contractor may assign this Agreement to an affiliate or in connection with any merger, reorganization, or sale of substantially all of Contractor's assets or other change of control transaction without any consent from the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach. Termination of the Master Agreement due to Contractor default may be immediate.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Parties acknowledge that they and their employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to other parties' and/or such other parties' clients/licensors. Any reports or other documents or items (including software) that result from the use of the Confidential Information by a party shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by receiving party) publicly known; (2) is furnished by disclosing party to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in receiving party's possession without the obligation of nondisclosure prior to the time of its disclosure

under this Master Agreement; (4) is obtained from a source other than disclosing party without the obligation of confidentiality, (5) is disclosed with the written consent of disclosing party or; (6) is independently developed by employees, agents or subcontractors of receiving party who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Receiving party shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Receiving Party shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Receiving party shall use commercially reasonable efforts to assist disclosing party in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, receiving party shall advise disclosing party immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and receiving party shall at its expense cooperate with disclosing party in seeking injunctive or other equitable relief in the name of disclosing party or receiving party against any such person. Except as directed by disclosing party, receiving party will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, receiving party shall turn over to disclosing party all documents, papers, and other matter in receiving party's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Parties acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to disclosing party that is inadequately compensable in damages. Accordingly, disclosing party may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Disclosing party acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement; provided that for the avoidance of doubt such indemnity shall not apply as relates to the design or functionality of the Services or the Products.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, any intellectual property indemnity claims under this section are not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. The minimum acceptable limits shall be as indicated below, with any deductible paid by Contractor, for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate (or the equivalent with an umbrella policy);

(2) CLOUD MINIMUM INSURANCE COVERAGE: Contractor shall maintain data breach and privacy/cyber liability coverage, including technology errors and omissions with a limit of $10 million per occurrence and in aggregate.

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

c. Contractor shall pay premiums on all insurance policies.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a

written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) includes the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the included Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the

Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of

Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff")

who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period

of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data

privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at Contractor's then applicable professional services rate or as otherwise mutually agreed to by the parties. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed

by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint

eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report

includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a

location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall within 48 business hours notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions

taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, to the extent a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request and at the expense of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report summary upon request to a Purchasing Entity and execution of an NDA. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with

a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the

removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Software as a Service (SaaS)

1.2 Risk Categorization.

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
SaaS	X	X		Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: WellSky Corporation

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Software as a Service (SaaS)

SaaS Minimum Discount % Off

Description	Discount
SaaS Minimum Discount %*	5.00%

* applies to all OEM's offered within this SaaS model

Additional Value Added Services

Item Description	Onsite Hourly Rate		Remote Hourly Rate	
	NVP Price	Catalog Price	NVP Price	Catalog Price
Maintenance Services	187.50	197.00	187.50	197.00
Professional Services	187.50	197.00	187.50	197.00
Deployment Services	187.50	197.00	187.50	197.00
Integration Services	187.50	197.00	187.50	197.00
Consulting/Advisory Services	187.50	197.00	187.50	197.00
Architectural Design Services	187.50	197.00	187.50	197.00
Statement of Work Services	187.50	197.00	187.50	197.00
Partner Services	187.50	197.00	187.50	197.00
Training Deployment Services	187.50	197.00	187.50	197.00
Post-Implementation Service Packages				
Managed Upgrade Services	5% Discount	Depends on Scope	5% Discount	Depends on Scope
Annual Wellness Checks	5% Discount	Depends on Scope	5% Discount	Depends on Scope
System Administration Services	5% Discount	Depends on Scope	5% Discount	Depends on Scope
*Travel costs for implementation and professional services to be billed separately				

	Deliverable Rates	
	NVP Price	Catalog Price
N/A		
N/A		

The State of Utah Division of Purchasing in conjunction with NAPSO ValuePoint

Technical Response to Utah Solicitation Number SK18008 NASPO ValuePoint Master Agreement for Cloud Solutions

July 6, 2018

Technical Response

This section should constitute the Technical response of the proposal and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

Mediware offers a variety of SaaS Cloud Solution modules to assist Human Services agencies to manage the services they provide and/or pay for. Mediware's interoperable solution modules support the entire eco-system of care from state and federal funders and oversight entities to local coordinating agencies to networks of service providers and to consumers of services and their families and caregivers.

With Mediware's solutions, customers manage multiple programs and funding sources in a single system centered on a global consumer record. These solutions allow organizations to:

- Enable comprehensive, cross-program care planning and delivery
- Eliminate program silos
- Support lifespan care models that cross multiple programs as consumers age or needs change

Mediware's solutions help customers improve care quality and consistency by encouraging communication and collaboration between care team members. Customers can realize the following results:

- Optimize outcomes
- Decrease administrative tasks
- Minimize fraud and abuse
- Enable truly coordinated care

Mediware solutions provide a number of benefits to our customers that are germane to their business needs and specific programs and populations served. Much of Mediware's customer base serves people with disabilities and the aging, helping them access community-based long-term services and supports that enable these people to live and thrive in their communities. Mediware's SaaS product modules include support for:

- Medicaid Waiver Management
- No Wrong Door/Single Entry Points

- Intellectual/Developmental Disability services
- Aging Services programs, including Older Americans Act funded programs
- Behavioral Health programs
- Aging and Disability Resource Centers
- Adult Protective Services
- Long-Term Care Ombudsman programs/Nursing Home Complaints
- Critical Incident Management
- Business Intelligence and reporting

Mediware's solutions help customers increase efficiency, reduce duplicate data entry, improve quality of the data they collect, and optimize the use of scarce resources to serve their clients. Mediware's solutions also allow customers to make use of the data they collect to improve services and demonstrate effectiveness to funders.

Mediware's solutions are deployed on Mediware's private cloud infrastructure and accessed by customer users over the internet. Mediware provides implementation, technical, and training services to effectively deploy its solutions to customers, tailoring the highly configurable solution modules to customers' business needs and requirements. Mediware's solutions are also interoperable, allowing connection and data sharing with customers' existing IT solutions. Mediware's implementation services include:

- Project Management
- Requirements Gathering/Solution Mapping
- Configuration
- Interface design, configuration, and deployment
- Data migration
- Testing and Validation
- Training
- Deployment and Go Live Support

Mediware's approach is collaborative with the customer and anticipates deep engagement with a customer project team to tailor the SaaS solution modules to the organization's specific business rules, workflows, policies, and procedures as they can be supported within the capabilities of the solution. In addition to purpose-built, best-of-breed modules for specific human services business areas, Mediware's approach relies on the use of built-in configuration utilities to tailor the solution's innate functionality to meet the unique requirements of the customer. Mediware also trains customer personnel to use these tools to maintain and update the system as needed.

Mediware's SaaS subscription model entitles customers to ongoing hosting, technical

and product support, product maintenance, updates, backup, and disaster recovery. Mediware's solution updates deliver not only defect corrections, but also product enhancement designed from input by our large customer base and by examination of the market and approaching trends. Customers are not stuck with a static system, but can enable additional features and new functions throughout their subscription period.

Mediware's SaaS infrastructure and support approach are detailed in Section 8 below. Mediware solutions support more than one thousand customer organizations and tens of thousands of users serving millions of consumers. In addition to their functional capabilities, Mediware's SaaS solutions are trusted for their security, availability, and scalability.

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

8 Technical Requirements

If applicable to an Offeror's Solution, an Offeror must provide a point by point response to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

8.1 (M)(E) Technical Requirements

8.1.1 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

Mediware complies with the requirements of Attachments C & D as applicable to the Software as a Service models as defined by NIST 800-145, providing purpose-built, interoperable COTS human services software solution modules. The SaaS modules Mediware proposes include the following elements, though these capabilities may appear in one or more of the proposed modules and may be limited to specific functions as appropriate to each individual module:

- Citizen Relationship Management
- Care Management
- Service Plans
- Assessments
- Analytics
    - Advanced Reporting
    - Business Intelligence
- Business Continuity/Disaster Recovery is provided as part of the services delivered through the Software as a Service Model
- Cloud and Infrastructure Management Services are included
- Collaboration elements are embedded into carious functional elements o f the solution offering
- Data Management
- Electronic Records Management
    - Finance
        - Assume Accounts Payable / Receivable
        - General Ledger
    - Budget

- Office Productivity Integration as part of the Mediware SaaS solution
  - Word Processing
- Security

8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of **Attachments C & D**.

Mediware is willing to comply with the requirements of Attachments C and D as they apply to the SaaS Cloud Solutions offered in this proposal.

8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in **Attachment D**.

Mediware's offerings adhere to the following services, definitions, and deployment models as identified in the Scope of Services in Attachment D:

Mediware is a cloud based services provider and has acquired and manages the computing infrastructure required for providing the SaaS solutions offered. Mediware runs the cloud software that provides the services, and makes arrangement to deliver the cloud services to customer organizations through network access.

Categorization of Risk

Mediware has the ability to store and secure Low Risk Data and Medium Risk Data as defined in FIPS Pub 199.

Services and Models

Mediware's offered services follow the NIST definition of cloud computing found in NIST Special Publication 800-145. Mediware's solutions conform to the five essential characteristics, outlined by 800-145 as they related to SaaS offerings.

- **On-Demand Self-Service:** Mediware's SaaS solutions are on-demand self-service services in that they are administered and operated by customer agencies and users without human interaction with Mediware personnel. While customers do not unilaterally provision computing capabilities, such as server time and network storage, these resources are available automatically as part of the SaaS offering.

- **Broad Network Access:** Mediware solutions are available over the network and accessed through standard mechanisms through a web browser and modules are available on mobile devices, tablets, laptops, and workstations.

- **Resource Pooling:** Mediware's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Customers generally have no control or knowledge over the exact location of the provided resources including storage, processing, memory, and network bandwidth.

- **Rapid Elasticity:** Mediware's resources including storage, processing, and memory are elastically provisioned and released to scale rapidly outward and inward commensurate with demand. To customers these capabilities often appear to be unlimited and are available as needed at any time.

- **Measured Service:** Mediware's SaaS solutions are offered in a private cloud infrastructure that automatically controls and optimizes resource use by leveraging metering capabilities such as storage, processing, bandwidth, and active user accounts. Resource usage is monitored, controlled, and reported, as necessary, to provide transparency for both the provider and Mediware's customers.

Offered Cloud Service Model

Mediware offers SaaS solutions that allow customers to use Mediware's Human Services software application modules on a cloud infrastructure. The applications are accessible from various client devices through a Web browser or a mobile app. Customers do not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for application configuration settings available through the built-in administrative and configuration utilities.

Deployment Method

Mediware's cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple business units and/or individual named users. The cloud infrastructure is owned, managed, and operated by Mediware, using third party data center partners.

8.2 (E) Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Mediware will provide the proposed SaaS cloud services directly. Mediware's solution uses a variety of third party products and services, but none of these third parties would be considered subcontractors to any engagement under the RFP.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Mediware does not intend to use subcontractors in any role under this RFP.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Mediware does not intend to use subcontractors in any role under this RFP.

8.3 (E) Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

Mediware agrees to report to the customer under the Master Agreement any use or disclosure of the Protected Health Information not provided for by the BAA of which it becomes aware.

Mediware shall notify the customer within 48 business hours of a confirmed breach of the Privacy Rule relating to the impermissible use or disclosure of Protected Health Information provided to the Mediware for purposes of carrying out its obligations under the Agreement. Unless otherwise required by law or agreed to by the parties, it shall be the responsibility of the customer to communicate with affected individual(s), the Secretary of HHS and the media information regarding the unintended use or disclosure. As necessary, Mediware shall provide data/analysis to support breach reporting and investigation.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Mediware's SaaS offerings do not include adware, software, or marketing. Mediware will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Mediware provides non-production environments as needed during the implementation phase, as follows:

- Test - Customer facing site used for testing configurations and deployment of test builds (application versions) during implementation period. This site may also be used for integration testing. If it is a multi-phased project and/or data conversion is part of the scope, Mediware will provide a data conversion instance, and other instances as needed during the implementation period.

After go live, Mediware provides two application instances, including:

- Test—This site is used for all non-production activity, including testing new builds and can be refreshed from production data to validate the new build. This is also used for testing configuration changes after go live.
- Live—Production system.

These environments are segregated at the database level.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

Mediware performs testing and validation on its SaaS offerings using different tools to comply with the Americans with Disabilities Act (ADA), Section 508 of the Rehabilitation Act. As part of this process, we generate a Voluntary Product Accessibility Template (VPAT) that contains information on our compliance with the Section 508 standards. Mediware's VPAT can be provided upon request.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

Mediware's SaaS solutions proposed are fully compatible and tested extensively with Internet Explorer 11. Other browsers are generally compatible with most areas of the

SaaS solutions designed for trained users (i.e. not the public), though known issues have been identified. Mediware has work planned on its product roadmap to continue to improve compatibility for these browsers. Mediware also offers mobile solutions for completing assessments out in the field and public-facing modules for collaboration with service consumers and their caregivers. These applications are fully compatible with the current versions of Chrome, Internet Explorer, Firefox, and Safari.

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Mediware shall meet with the Purchasing entity to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations. As a matter of course, Mediware executes a Business Associate Agreement (BAA) with all customers to set forth the obligations for each part regarding to protection of Protected Health Information (PHI) and Personally Identifiable Information (PII). The BAA is aligned to HIPAA/HITECH regulations and best practices in the health care industry.

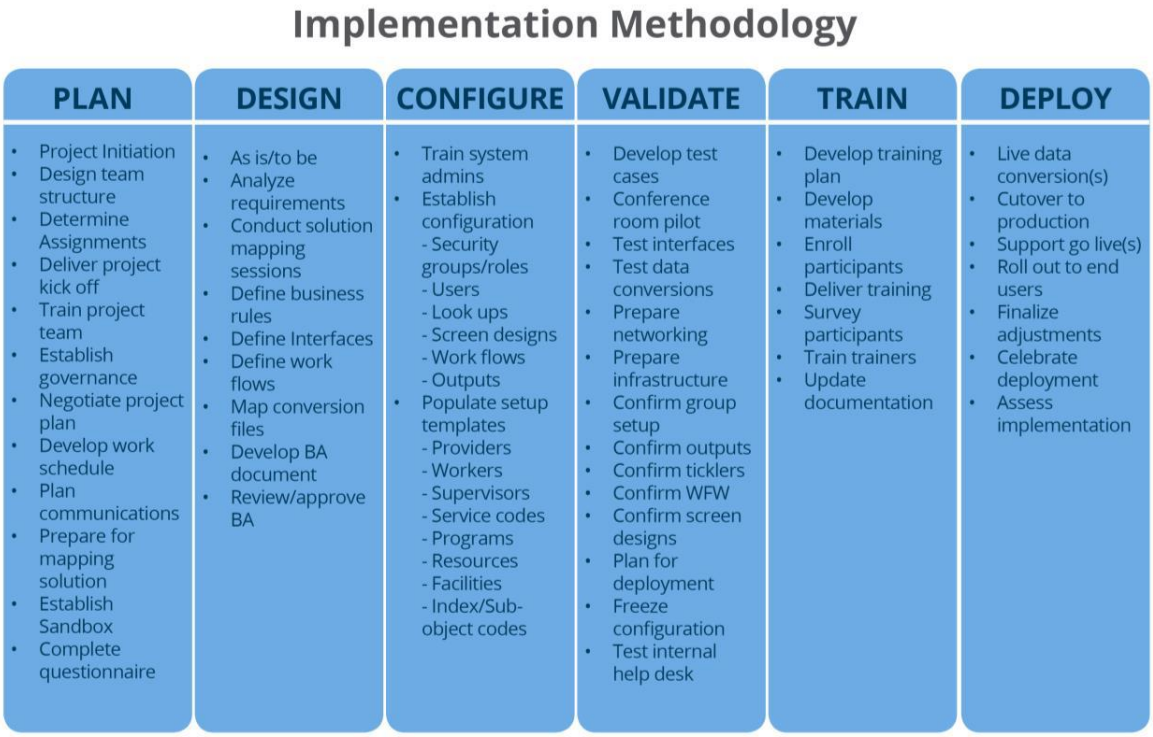
8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Mediware has experience with a number of approaches to deploy its solution across several lines of business. The preferred approach depends on several factors, including:

- specific business requirements, including business process/workflow
- timeline drivers and deadlines
- availability of customer project resources, including subject matter experts, technical resources, training resources, etc.

Sometimes, Mediware suggests a phased approach to deploy one or more lines of business in sequential phases. Another approach is to deploy common business functions across the several lines of business simultaneously and roll out functionality to functional groups of users or roles

Mediware's Implementation Methodology involves six primary processes that are executed in multiple iterations as needed to complete the solutions delivery. These are shown in the diagram below.



The methodology is overlaid with industry-standard project management practices to ensure effective communication, risk management, organizational change management, and cost control.

Integrated throughout the project lifecycle is Organizational Change Management, a continual process of two-way communication with stakeholders. Our implementation approach takes into account the challenges of such comprehensive projects, including:

- Generating a common understanding and agreement on system and business requirements so that stakeholders can and want to support the new system.
- Building a guiding coalition of the organization's leaders at all levels to drive agreement and action.
- Engaging stakeholders throughout the life of the project to sustain interest, participation, and commitment.
- Analyzing workforce impacts and training requirements to prepare all end users to successfully operate in a new environment.
- Delivering training to impart new technology and process skills across a geographically dispersed user population.

- Identifying and mitigating project and implementation risks related to stakeholder involvement and buy in.

Mediware is fully prepared to staff, manage, control, and execute projects so as to move customers toward their transformation goals with great software delivered right on time and within budget, as planned. Mediware's approach to project management is to shape the plan for getting users into the system early in the project's life cycle, and then help them adjust quickly and successfully to the new model of operations as additional functions and features are deployed over time. This approach ensures that earned value begins to accrue very rapidly.

A key goal of the project management approach is to begin with, and thereafter sustain, high levels of performance throughout the life of the initiative. We will get off to a productive start and demonstrate progress toward deployment in short order. To achieve these results, the project management approach will reflect strong leadership and effective, positive communication that conveys a collaborative spirit within the need for "running a tight ship." Mediware's methodology drives the project team to hold periodic discussions about upcoming events, to identify the milestones and targets that keep the initiative on track, and to continually reassess how best to achieve a successful completion.

8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.
- How Offeror will maintain discounts at the levels set forth in the contract.
- How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.
- How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.

Mediware expects to update its SaaS Cloud Services product modules regularly. Mediware's SaaS subscription entitles customers to product updates while they are subscribed. Updates are designed to ensure that current functionality is fully retained and that activation of any enhanced functionality has minimal impact to current use by the customer. Mediware apprises customers of updates several weeks prior to release and works with customers who may be unavoidably impacted negatively by any update to provide mitigation as needed.

Any new services or updates to existing services that Mediware introduces will meet the minimum specifications and terms and conditions outlined in the resulting master agreement and in Mediware's response to the RFP. If any new services are added with accompanying terms and conditions, these will not diminish or weaken existing terms and conditions. For updates, Mediware will utilize the same pricing structure as was used for services originally contracted. For new services, Mediware reserves the right to offer novel pricing structures in accordance with reasonable business practice and market trends. Mediware will offer the same minimum discount prices identified in this proposal to the updated solutions and services.

8.4 (E) Customer Service

8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

Mediware manages its product engineering, professional services, SaaS solution support, and customer support services with excellence in mind. Mediware is focused on providing high quality products and delivering them in ways that delight customers.

Mediware has adopted the following Quality Policy:

> *Put quality first by maintaining and continuously improving the quality of our operations, products, and services so as to meet regulatory requirements, product specifications, and customer needs. Through this effort Mediware can provide safe, effective, and reliable technology to assist our customers' healthcare endeavors.*

Mediware knows its continued success depends entirely on its ability to satisfy customers' needs. That's why Mediware, with the help of our customers and our teams of subject matter experts, have introduced a number of programs designed to help customers maximize the value of their investments in Mediware technologies.

Satisfaction Surveys

Because customer satisfaction is a critical component of Mediware's ongoing business success, customers are surveyed quarterly for their feedback and Mediware actively monitors satisfaction rates.

To maintain the high levels of quality customers deserve, Mediware has implemented internal programs to reward employees, project teams, and departments for their contributions to customer success.

This program reinforces our core principles:

- **C**ustomer support
- **A**ccountability
- **R**espect
- **E**xcellence

Each quarter, employees who contribute to customer successes are rewarded for their outstanding efforts.

Success First

This program provides enhanced project management training, rigorous customer support processes, and focused attention from dedicated account managers for all customers so that each one has the information and training needed to successfully use their software solutions.

Zero Defects

As part of this program, Mediware made a significant investment in internal training to establish consistent, reliable, and repeatable product development and testing processes with regular quality checks across all our product lines. Mediware also provided advanced training on specification definition and testing as well as new automated tools and additional staff for quality assurance.

Mediware's Customer Support procedures include escalation paths for defects and for customer complaints up to the highest levels of the organization.

Mediware provides an Availability SLA, included with our response (filename: "Mediware SLAs.pdf") as well as a support SLA included in our standard Master License and Service Agreement (file name: "Mediware Master License Agmt.pdf").

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

c. Customer Service Representative will respond to inquiries within one business day.

d. You must provide design services for the applicable categories.

e. You must provide Installation Services for the applicable categories.

Mediware provides implementation services for all its SaaS solutions that include the configuration and deployment services as outlined in 8.3.7 above. Mediware's SaaS solutions are based on Commercial-Off-the-Shelf (COTS) products and are not custom-developed. Mediware does not provide design services per se, but Mediware's solutions have extensive configuration tools that allow customers to define application behavior, business rules, workflow, data, and appearance.

As part of its SaaS service offerings Mediware's offers 24/7/365 monitoring of the hosting environment and user experience. Mediware also provides ongoing solution support. The Mediware Customer Support team is purposed to ensure successful use of Mediware's SaaS solutions, with dedication to providing outstanding product support to customers. Mediware's support team provides telephone, email, and Internet-based support. All customer inquiries are logged as cases in Mediware's Support Center CRM system and assigned unique identification numbers for tracking.

The Mediware Customer Support Team includes experienced Customer Care Analysts (CCAs) with extensive technical expertise and ongoing training in all Mediware applications and customer business processes. Mediware CCAs focus on responding to customers' support needs quickly and accurately, with the goal of consistently exceeding customers' expectations.

Mediware's support plan provides the ability for customers to submit support cases through several methods: the online Mediware Customer Portal, by telephone, or by email for Mediware Customer Support assistance during standard business hours (8 am-9 pm ET). Customers may also submit support cases through these methods 24x7 outside of business hours, and the Mediware Support Team will follow-up during normal business hours. The support organization is dedicated customer assistance and will provide help in many areas, such as answering user questions, logging system

enhancement requests, handling patch and update notifications, and providing assistance in troubleshooting problems.

Contact and Case Creation Methods

The support team business processes and data recording utilize the support case record. All assistance provided is recorded in the case as it is tracked through the various stages to completion. Mediware advises customers to always create a support case whenever a response is needed from Mediware Customer Support.
Mediware offers three methodologies to create support cases:

1. Mediware Customer Support Portal
2. Email – customersupport@mediware.com
3. Phone Support - 1-800-318-7260

Mediware Customer Support Portal

The Mediware Customer Portal is an automated solution for system administrators to manage support tickets. The portal provides system administrators an online tool to create and manage cases with the Mediware Customer Support team. Mediware Customer Support uses customer information provided through the portal to understand and effectively respond to customer needs, streamline and simplify support efforts, improve customer satisfaction, and improve abilities to manage Mediware support requests in a timely and effective manner. Through the portal, system administrators have around-the-clock access to real-time status of their submitted support cases.

Email:

Sending an email to the Mediware Support Team email address will automatically generate a support case in the CRM system. Users may email Mediware at any time at customersupport@mediware.com and the Mediware Customer Support Team will communicate with the customer, including through use of the case reporter, through the case record. Users will receive a response in their inbox and may reply via the email thread throughout the support case life cycle. All email activity is stored within the case record.

Phone:

Mediware provides toll-free telephone-based support to customers, recognizing that not all incidents are easily communicated by online case entry alone. Phone support is suggested for situations where customers have difficulty articulating a need via the Customer Portal or if they need to speak directly to a support representative during business hours. Mediware Customer Care Analysts answer incoming calls as designated in a queue to facilitate user responsiveness.

Remote Session Sharing Tools

Mediware also provides a collaborative, web-based access tool to allow sharing of desktops between support representatives and end users during phone conversations. This ability to demonstrate and view enables Mediware to provide an interactive support experience that further contributes to an interactive customer experience. In addition to walking through illustrative examples and results of their analyses, the support team can use the tool to shadow customer user sessions to further understand the question or problem under consideration. This tool enables the support team to:

- Accelerate diagnosis and problem solving.
- Troubleshoot issue on customer hardware and solutions when needed.
- Provide real-time analysis while a problem is occurring.
- Demonstrate product features when appropriate.

After Hours Case Submission Support

The Mediware Customer Support Portal, email support, and phone-based case reporting (to voice message) are all available methods to log cases after hours. 24 x 7, Customers can use the portal to report/view support cases, and may report cases via the portal, email, and phone methodologies. Mediware Customer Support will follow-up on cases submitted after-hours during normal business hours.

Mediware also has 24/7 monitoring of the entire hosting infrastructure and responds to critical alerts after hours. Typically, if a customer were to encounter a critical hosting issue, Mediware would already be aware and have begun to isolate, troubleshoot and resolve.

Mediware provides a support SLA based on issue severity. This information is provided in Mediware's Master License and Service Agreement attached to this submission (file name: "Mediware Master License Agmt.pdf"). This information is not reprinted here for brevity.

8.5 (E) Security of Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Mediware understands that certain information about our customers' patients is private and personal. Mediware is committed to protecting the privacy of that information pursuant to the legal standards created by the Omnibus Final Rule, Health Insurance Portability and Accountability Act of 1996 (HIPAA), section13404 of the Health Information Technology for Economic and Clinical Health Act (HITECH) of the American Recovery and Reinvestment Act of 2009 (ARRA). Mediware has implemented, as applicable, comprehensive Privacy and Security policies and procedures, with the intent to adequately and appropriately protect the confidentiality, availability and integrity of customers' data.

Mediware follows a comprehensive, multi-level security program to ensure integrity and protection of customer data from unauthorized access. Mediware's program is based on an organizational commitment to the security of customer data and regulatory compliance with HIPAA. Our security program consists of technical measures and is complemented by internal operational policy and procedures.

System and Application Security

Mediware applications provide role-based security, which facilitates compliance with HIPAA and HITECH privacy and security standards.

Protected consumer/participant data is contained exclusively within customer-specific databases that are accessible only by customer-authorized users. Each user is authenticated, and password complexity is enforced by customer system administrators via the system utilities. Roles can be configured to control access to each area of the *Mediware* application.

At the application level, Mediware solutions provide robust organizational- and role-level security that allows for very granular security management. Mediware's configurable application security infrastructure controls which functions a user can access as well as what data a user can access down to the field level.

Mediware' s role-based security allows a System Administrator to create groups that define the application modules, and fields that will be available to users in a specific division or functional business area (e.g., finance) and roles that define further refine the areas of the application available to users with specific job functions, and their edit

privileges (e.g., view, add, edit, delete, etc.). These features allow an organization to define an unlimited number of roles to help ensure that users are able to access data appropriate to their line of business and job function.

Mediware Security Policies and Procedures

Mediware has a comprehensive set of internal corporate HIPAA policies, including access control policies and procedures to secure PHI. These policies include an approach that provides access to data only by essential personnel according to job requirements. All employees complete annual HIPAA training. Below are some highlights of the HIPAA policies and procedures now in place at Mediware:

- Mediware maintains on staff a Chief Security Officer, responsible for developing, monitoring, and enforcing security practices, including implementation of policies and procedures to prevent, detect, contain, and correct security violations.
- Response protocols in the event of an emergency or other occurrence that damages systems that contain EPHI, including data backup plan, DR plan, emergency mode operation plan, testing, and revising procedures.
- Mediware screens all personnel by performing reference and background checks, and by requesting information about a candidate's former work and, if any, criminal history.
- All Mediware employees, contractors, and sub-contractors are required to read, understand, and abide by Information Security policies including those noted above, and are trained at least annually on the following requirements:
    - Protect PHI/PII - All Mediware employees, contractors, and sub-contractors are required to protect sensitive data from accidental or intentional unauthorized access, modification, disclosure, or destruction.
    - Report Violations - All Mediware employees, contractors, and sub-contractors are required to report any known or suspected violations and/or security concerns to management, Information Security, or the HIPAA Privacy Officer. All Mediware employees, contractors, and sub-contractors are required to report faulty physical controls/equipment (shredders, door locks, etc.) as well.

Mediware SaaS Operations Security

Below are some of the services provided as part of the Mediware SaaS solution:

- Anti-Virus: Up to date, automated real-time antivirus scanning;
- Firewall management/monitoring;
- Hosting in a SSAE-16 SOC I and SOC II Audited Data Centers;
- Perimeter defense at the network edge with firewall architecture and port/IP blocking to guard against unknown/unnecessary protocols and/or traffic from entering the production network;

- Deploying and maintaining antivirus software, operating system patches, hardware, firmware patches/upgrades;
- Routine review of system logs for security issues on network hardware and perimeter devices;
- Maintenance of Windows security group policies to prevent unnecessary execution of applications/activities in our hosted solution environment;
- User authentication to assure that users are properly authenticated in the network environment;
- User application security roles that allow access only to customer designated system resources and data based.
- Limited access to hosting infrastructure enforced by facility security system
- Regularly scheduled patching and security updates to the operating system, application, core network infrastructure
- Data is encrypted in transport using a third-party SSL/TLS certificate, employing 2048-bit keys for digital signatures, and Counter with Cipher block chaining mode (CCM), with AES-256 for message authentication and a SHA2-256-bit hash for secure hashing.
- Data is encrypted at rest on disk for both OLTP databases and database backups using AES-256-bit encryption; and
- Off site, secure storage of encrypted database backups.

Mediware Security Tools

Mediware provides the following security measures in the hosting environment:

Security Measure	Security Objective	Vendor
Two Factor Authentication	Assure administrator access to hosting environment is controlled by additional authentication method.	Duo Security
Intrusion Detection/Prevention	Network based IDS/IPS based on Snort and Bro	Bricata
Centralized Log Management	Single source of security event logging Tenable Log Correlation Engine as part of Tenable Security Center Continuous View	Tenable
File Integrity Monitoring	Detect/remediate unauthorized change on hosting infrastructure file system Tenable Security Center Continuous View	Tenable
Vulnerability Scan	Detect operating system	Tenable Nessus

	vulnerabilities and prioritize risk and remediation	
Antivirus	Scanning system for virus and malware protection	Kaspersky
AES 256-bit encryption	Encryption of transactional data at rest for OLTP	Pure Storage
FIPS 140-2 encryption	Encryption attachment data at rest in a separate database on separate storage.	Winchester Systems
CommVault Simpana	Encrypted off-site backup for customer data (FIPS 140-2 Certified Encryption).	CommVault
File transfer encryption FTP/SFTP/FTPS	Transport encryption for file movement between Mediware SaaS and customer systems	SolarWinds ServU FTP
HTTPS	Encrypted data transport, currently at TLS.1.1 and 1.2	IIS 3rd party Certificate
Network Firewalls	Restriction of port access into SaaS network	Cisco ASA 5515x
Identity Management	Authentication of end users and federated single sign on	Microsoft Active Directory/Active Directory Federation Services
Active Directory Audit	Active Directory Audit/Reporting of Mediware SaaS environment	Manage Engine
Windows Patching	Maintain all critical and important security patches on operating system in Mediware SaaS environment.	Windows Security Updates Services

Mediware regularly evaluates third party tools and services to support the Mediware SaaS environment and these tools are subject to change.

Physical Security

Facility entry is monitored with security cameras providing 24x7x365 electronic video surveillance of entry and exit to and from the hosting facility. Data centers are Facility are masonry constructed with ballistics resistant glass. Access to the data center and hosting facility equipment is controlled by on site staff 24x7x365. Mediware employees must check in with facility security, sign a security log, and present valid government identification. Facility security staff then validate access is granted for the individual.

Mediware staffs are then assigned a security badge and escorted by facility security to the Mediware cabinets. Facility security staff then unlocks the Mediware assigned cabinets and grants access. All customer data and equipment is stored in locked cabinets and keys to these cabinets are provided only to the authorized personnel.

Equipment Security

Equipment is physically protected from security threats and environmental hazards. All hosting facility equipment is stored in locked cabinets. Keys are provided to the authorized personnel only.

- **Power Supplies.** The power supplies of the hosting facility equipment on which customer data is located are stored in locked cabinets. Keys are provided to authorize personnel only.
- **Cabling Security.** The network cabling located in each rack of the hosting facility equipment are stored in locked cabinets. Keys are provided to authorize personnel only.
- **Equipment Maintenance.** Mediware personnel perform equipment maintenance in secure areas in the hosting facility or transport systems to Mediware corporate offices for maintenance. In the rare circumstance requiring equipment outside of the hosting facility, Mediware encrypts all customer data using AES-256 Bit encryption.
- **Off-Premise Equipment.** All non-production hosting equipment is stored in a Mediware facilities, protected by electronic key card access systems.
- **Secure Disposal.** All media containing customer data is destroyed securely by a NAID certified third party vendor. As needed, Mediware provides a full accounting including a certification of secure destruction and a full inventory of the media destruction by serial number.

Production Change Management

Software changes or software updates deployed in our SaaS environment is managed by our change control process. Mediware ensures integrity of the operating environments. Change to actual source code is managed through our source code management tool and audit/build reports that describe exactly what was modified in the repository as well as any given build of the software package. Also, only certain individuals based on their role are privileged to have access to the source code repository. Based on their role, users may not be allowed to make functional builds of the software. Mediware ensures that rogue builds are not created. Only authorized users are provisioned with accounts to Mediware system and the system forces users to authenticate before gaining access. Further, log in, check outs, changes and check-ins of all files is auditable. When authorized individuals leave the organization for any reason, our corporate employee exit procedures involve disabling the individual's account.

Security Architecture

The Mediware SaaS network is segmented into three logical networks as follows:

- **Application and Web Services:** Mediware network is isolated and contains all web/applications servers, including Internet Information Services and SharePoint Services, Active Directory Federation Servers, and load balancer virtual addresses. These servers and services are all provided private IP addresses. Public facing web services URLs are assigned a publicly routable IP address, which is mapped to a private LAN address. Web services addresses are allowed to communicate inbound and outbound on port 443. SFTP services are restricted to port 22 inbound on a public facing IP address and server, but cannot communicate with the LAN, except via a channel on port 1180 which is restricted to communications only with the public facing SFTP server.
- **Database Services:** All database servers are segments on a subnet which is isolated from the applications and web services subnet.
- **Management Subnet:** A management subnet is in place to allow remote administrative access to all server infrastructures. Mediware subnet is only accessible via SSL VPN or with direct console access.
- **Perimeter Security**: Mediware maintains redundant firewalls at the perimeter. These firewalls are configured to allow traffic on only ports 443/22 and those required for Citrix connectivity for Mediware applications delivered via the Citrix ICA protocol on port 443. The firewalls are configured to block all other traffic and enforce the network segmentation indicated above. The ports and communications between the isolated subnets are restricted to the minimal necessary ports and services to enable the Mediware SaaS application environment to function properly.

Auditing and Logging

Mediware provides application audit logs for each end user's access or modification of transactional data. The audit record identifies the user by unique system identifier, time and date of action, and the transactional data values before and after changes. Mediware audit information is readily available for reporting by authorized users and provides the necessary forensics to reconstruct data manipulation sequences over time and identify the user(s) who performed the manipulation.

In addition to the application logs provided in Mediware products, Mediware also monitors the production hosting environment for anomalies and error detection/correction. Logging is accomplished through a variety of third party and native tools. Examples include, but are not limited to:

- Internet Information Server logs;
- Custom application event logs;
- Windows Operating System event logs, and

- SharePoint logs

Vulnerability and Patch Management

Mediware conducts regular vulnerability scans for operating system vulnerabilities using third party vulnerability management scanners, including Microsoft Windows System Update Server and Kaspersky Systems Management module. These monthly results are remediated by the Mediware SaaS team as part of the SaaS maintenance schedule.

On a monthly basis, the Mediware SaaS Team Mediware applies critical and security updates to operating systems and third-party software in the Mediware SaaS environment. Mediware deploys critical Microsoft and other third-party service patches to the production environment each month, as follows:

Emergency patch procedures for security related issues:

Mediware monitors vendor alerts, trusted third party advisories, vulnerability reports, and other sources to identify valid security alerts/issues. The resultant service patches are introduced into our testing and quality assurance process and are introduced into our release schedule as they become available.

Mediware installs emergency security patches immediately if the patch is deemed so important by the vendor, or by industry experts, that without it the SaaS environment would be exposed to attacks, which threaten operational integrity. Every effort is made to install these patches during regularly scheduled maintenance windows, but in some circumstances these patches are necessary on an emergency basis without prior customer notification to prevent viruses in the wild or other high security risks. As necessary, Mediware can back out these patches through restoration of the operating system to its state prior to the patches.

Mediware tests all application deployments against the latest critical and important patches from Microsoft and tests and deploys critical and important patches for the entire Microsoft platform stack (OS/SQL//SharePoint) on which Mediware products are deployed.

Personnel Security

Mediware screens all personnel by performing reference and background checks, and by requesting information about a candidate’s former work and, if any, criminal background.

Security Training

All Mediware employees, contractors, and sub-contractors are required to read, understand, and abide by Information Security policies, and are trained at least annually on the following requirements:

- **Protect PHI/PII** - All Mediware employees, contractors, and sub-contractors are required to protect sensitive data from accidental or intentional unauthorized access, modification, disclosure, or destruction.
- **Training** - All Mediware employees, contractors, and sub-contractors are required to attend annual awareness training.
- **Report Violations** - All Mediware employees, contractors, and sub-contractors are required to report any known or suspected violations and/or security concerns to management, Information Security, or the HIPAA Privacy Officer. All Mediware employees, contractors, and sub-contractors are required to report faulty physical controls/equipment (shredders, door locks, etc.) as well.

Security Compliance & Audits

Mediware conducts various security audits of the Mediware SaaS platform infrastructure and associated SaaS applications. The audits generally consist of penetration and vulnerability scanning and a review of the architecture and operational practices and procedures performed by Mediware and its supporting third party vendors. Mediware takes aggressive action to address any issues or recommendations resulting from the audits. In addition, Mediware collaboratively works with customers who would like to conduct similar scans.

The above measures result in a comprehensive set of security tools and procedures that ensure the protection and security of customer data and the overall SaaS infrastructure. During the Software Development Lifecycle (SDLC), Mediware performs various levels of design reviews which include a security evaluations as appropriate. Mediware's security strategy is heavily influenced by widely recognized industry standard sources including:

- HIPAA Guidelines on Information Privacy and Security;
- HI-TECH;
- NIST Special Publication (SP) 800-53, Revision 4 Information Security Controls; and
- Open Web Application Security Project (OWASP);
- Independent audits.

Security validation continues to play an important role throughout implementation deployment. Before the system is placed into production, functional requirements, security requirements, default settings, and configured controls need to be verified through systems testing. Testing needs to verify that security requirements were

implemented as specified, that security controls work as intended, and that documentation has been developed for managing future changes to any of the system's security settings. Post cutover, re-testing of security should be performed before deploying updates and approved changes to the system's configuration. As an added measure, training curriculum normally includes security awareness recommendations to prepare the workforce to operate, support, and maintain the system with controls and protections in place for sensitive or private information. Training normally occurs after testing is completed and before access to the system is permitted.

Finally, we also consult our customers for their specific security requirements, and remain committed to evolving our security practices to meet the ever-changing security landscape.

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Mediware will comply with all material state and federal statutes, regulations and rules applicable to the services proposed, including those related to data privacy and security. Mediware's expectation is that any such contractual obligation shall be mutual. Mediware is committed to protecting the privacy of that information pursuant to the legal standards created by the Omnibus Final Rule, Health Insurance Portability and Accountability Act of 1996 (HIPAA), section13404 of the Health Information Technology for Economic and Clinical Health Act (HITECH) of the American Recovery and Reinvestment Act of 2009 (ARRA). Mediware has implemented, as applicable, comprehensive Privacy and Security policies and procedures, with the intent to adequately and appropriately protect the confidentiality, availability and integrity of customers' data.

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Mediware will not access a customer's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

8.6 (E) Privacy and Security

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in **Attachment D**, including supporting the different types of data that you may receive.

As outlined at length in Section 8.5.1 above, Mediware is fully committed to compliance with NIST and other relevant industry standards to support low risk and medium risk data as described in the Scope of Services. The information provided in Section 8.5.1 is not reprinted here for brevity.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Mediware uses the NIST Cyber Security Framework and has selected security controls based our risk assessment and the NIST 800-53, Revision 4, moderate baseline control set and therefore is in material compliance with FISMA as applicable to implementations which may result from this purchasing vehicle. As applicable, Mediware can assess compliance with NIST SP 800-171 and/or FIPS 200 to the extent that these controls exceed existing moderate baseline controls of NIST 800-53 implemented in the Mediware SaaS offering. Mediware does not collect credit card data or FTI and is therefore does not presently implement PCI controls, nor follow controls that are specific to IRS Publication 1075 and not already implemented by Mediware via NIST 800-53 moderate baseline controls selected.

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

In Section 8.5.1 above, Mediware has provided detailed description of the security practices in place to secure the data and the SaaS applications Mediware provides. This information is not reprinted here for brevity.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

In Section 8.5.1 above, Mediware has provided detailed description of the data confidentiality standards and practices that are in place to ensure data confidentiality in Mediware's solutions and its SaaS operations. This information is not reprinted here for brevity.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Per the original engagement with third-party auditors, Mediware received its annual re-certification SOC 2 Type II AT 101 and SOC 3 AT 101 Annual Re-Certification April 2017. The audit and evaluation cover the reporting periods of May 1, 2016 to April 30, 2017. As of the submission of this document, Mediware has just completed the audit and is awaiting the audit report results of the 2018 SOC 2 Type II audit.

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Mediware provides application audit logs for each end user's create, read, edit update of (access or modification) of transactional data. The audit record identifies the user by unique system identifier, time and date of action, and the transactional data values before and after changes. Mediware audit information is readily available for reporting by authorized users and provides the necessary forensics to reconstruct data manipulation sequences over time and identify the user(s) who performed the manipulation.

In addition to the application logs provided in Mediware products, Mediware also monitors the production hosting environment for anomalies and error detection/correction. Logging is accomplished through a variety of third party and native tools. Examples include, but are not limited to:

- Internet Information Server logs;
- Custom application event logs;
- Windows Operating System event logs, and
- SharePoint logs

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Mediware applications provide role-based security, which facilitates compliance with HIPAA and HITECH privacy and security standards.

Protected consumer/participant data is contained exclusively within customer-specific databases that are accessible only by customer-authorized users. Each user is authenticated, and password complexity is enforced by customer system administrators via the system utilities. Roles can be configured to control access to each area of the *Mediware* application.

At the application level, Mediware solutions provide robust organizational- and role-level security that allows for very granular security management. Mediware's configurable application security infrastructure controls which functions a user can access as well as what data a user can access down to the field level.

Mediware's role-based security allows a System Administrator to create groups that define the application modules, and fields that will be available to users in a specific division or functional business area (e.g., finance) and roles that define further refine the areas of the application available to users with specific job functions, and their edit privileges (e.g., view, add, edit, delete, etc.). These features allow an organization to define an unlimited number of roles to help ensure that users are able to access data appropriate to their line of business and job function.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Mediware undertakes the following notification procedures in the event of a security incident

- All Mediware employees and contractors are required to properly respond in a consistent manner, with appropriate leadership and technical resources, to an incident that threatens the availability, confidentiality and integrity of information resources.
- The Mediware Privacy/Security Official and IT Department is available to facilitate and provide guidance with for any security incidents that affect Mediware resources or threatens the availability, confidentiality and integrity of information. All security incidents involving PHI/ePHI, confidential or internal information must be reported immediately to the IT Department and the Privacy and Security Official
- Mediware defines an incident as any act that violates Mediware Privacy Practices or Information Security Policy and Practices, consistent with HIPAA. The types of activity below are common violations and are required to be reported immediately.
    - Unauthorized attempts (either failed or successful) to gain access to a system or data.
    - Unwanted disruption or denial of service
    - Unauthorized use of a system for processing or storing data
    - Inappropriate usage according to the acceptable use policy
    - Theft or loss of Mediware assets
- **Information Security Breach Notification** – A breach of unsecured PHI/ePHI or confidential information requires special handling.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Physical Security

Facility entry is monitored with security cameras providing 24x7x365 electronic video surveillance of entry and exit to and from the hosting facility. Data centers are Facility are masonry constructed with ballistics resistant glass. Access to the data center and hosting facility equipment is controlled by on site staff 24x7x365. Mediware employees must check in with facility security, sign a security log, and present valid government identification. Facility security staff then validate access is granted for the individual. Mediware staffs are then assigned a security badge and escorted by facility security to the Mediware cabinets. Facility security staff then unlocks the Mediware assigned cabinets and grants access. All customer data and equipment is stored in locked cabinets and keys to these cabinets are provided only to the authorized personnel.

Equipment Security

Equipment is physically protected from security threats and environmental hazards. All hosting facility equipment is stored in locked cabinets. Keys are provided to the authorized personnel only.

- **Power Supplies.** The power supplies of the hosting facility equipment on which customer data is located are stored in locked cabinets. Keys are provided to authorize personnel only.
- **Cabling Security.** The network cabling located in each rack of the hosting facility equipment are stored in locked cabinets. Keys are provided to authorize personnel only.
- **Equipment Maintenance.** Mediware personnel perform equipment maintenance in secure areas in the hosting facility or transport systems to Mediware corporate offices for maintenance. In the rare circumstance requiring equipment outside of the hosting facility, Mediware encrypts all customer data using AES-256 Bit encryption.
- **Off-Premise Equipment.** All non-production hosting equipment is stored in a Mediware facilities, protected by electronic key card access systems.
- **Secure Disposal.** All media containing customer data is destroyed securely by a NAID certified third party vendor. As needed, Mediware provides a full accounting including a certification of secure destruction and a full inventory of the media destruction by serial number.

Security Architecture

The Mediware SaaS network is segmented into three logical networks as follows:

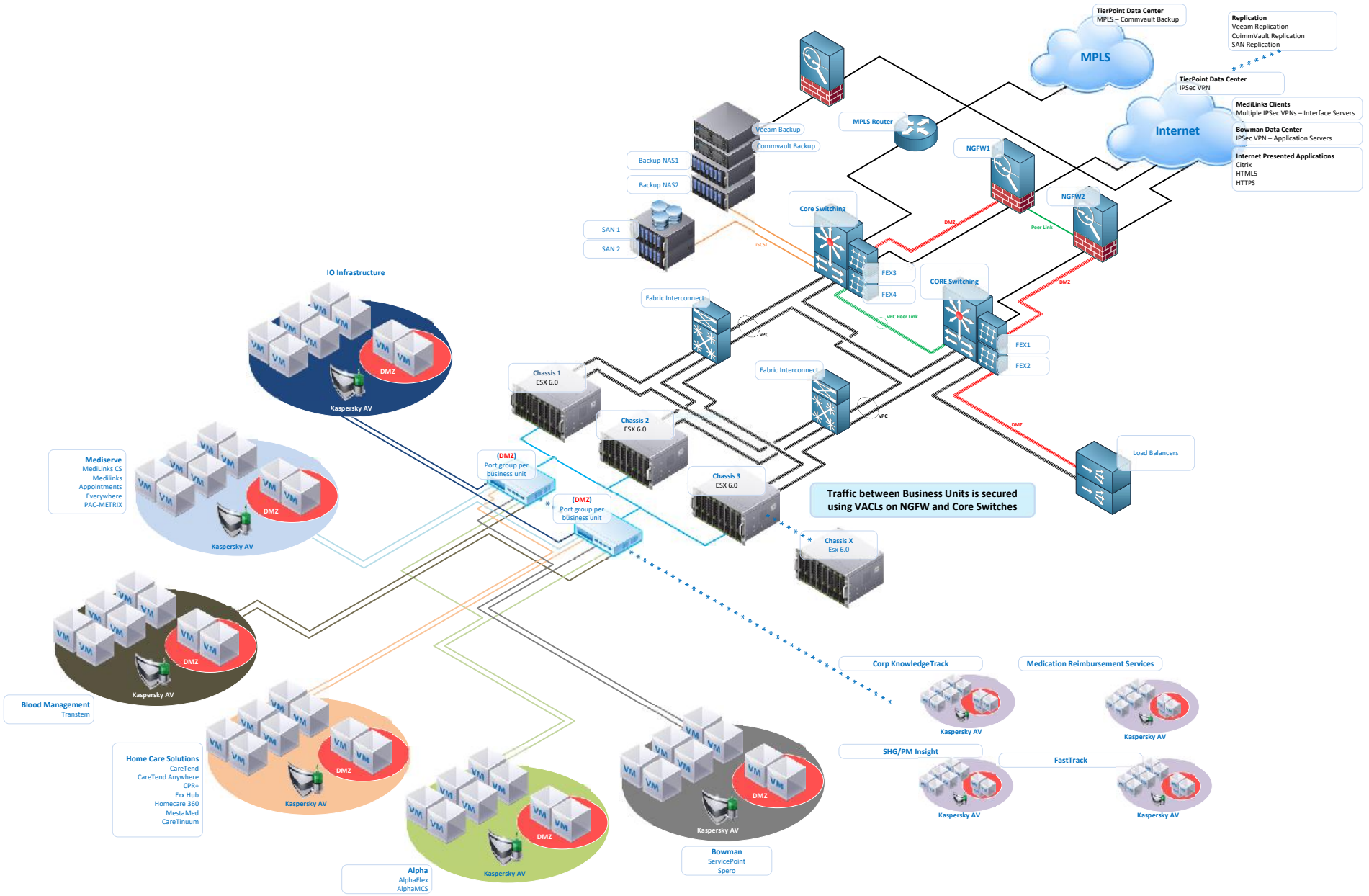
- **Application and Web Services:** Mediware network is isolated and contains all web/applications servers, including Internet Information Services and SharePoint Services, Active Directory Federation Servers, and load balancer virtual addresses. These servers and services are all provided private IP addresses. Public facing web services URLs are assigned a publicly routable IP address, which is mapped to a private LAN address. Web services addresses are allowed to communicate inbound and outbound on port 443. SFTP services are restricted to port 22 inbound on a public facing IP address and server, but cannot communicate with the LAN, except via a channel on port 1180 which is restricted to communications only with the public facing SFTP server.
- **Database Services:** All database servers are segments on a subnet which is isolated from the applications and web services subnet.
- **Management Subnet:** A management subnet is in place to allow remote administrative access to all server infrastructures. Mediware subnet is only accessible via SSL VPN or with direct console access.
- **Perimeter Security**: Mediware maintains redundant firewalls at the perimeter. These firewalls are configured to allow traffic on only ports 443/22 and those required for Citrix connectivity for Mediware applications delivered via the Citrix ICA protocol on port 443. The firewalls are configured to block all other traffic and enforce the network segmentation indicated above. The ports and communications between the isolated subnets are restricted to the minimal necessary ports and services to enable the Mediware SaaS application environment to function properly.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

Mediware is pleased to provide a Security Reference Technical Architecture supporting Mediware's SaaS Cloud Services offerings on the page following. Page numbering is non-sequential.

Mediware at IO Data Center

Logical Network Diagram



8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Mediware Security Policies and Procedures

Mediware has a comprehensive set of internal corporate HIPAA policies, including access control policies and procedures to secure PHI. These policies include an approach that provides access to data only by essential personnel according to job requirements. All employees complete annual HIPAA training. Below are some highlights of the HIPAA policies and procedures now in place at Mediware:

- Mediware maintains on staff a Chief Security Officer, responsible for developing, monitoring, and enforcing security practices, including implementation of policies and procedures to prevent, detect, contain, and correct security violations.
- Response protocols in the event of an emergency or other occurrence that damages systems that contain EPHI, including data backup plan, DR plan, emergency mode operation plan, testing, and revising procedures.
- Mediware screens all personnel by performing reference and background checks, and by requesting information about a candidate's former work and, if any, criminal history.
- All Mediware employees, contractors, and sub-contractors are required to read, understand, and abide by Information Security policies including those noted above, and are trained at least annually on the following requirements:
    - Protect PHI/PII - All Mediware employees, contractors, and sub-contractors are required to protect sensitive data from accidental or intentional unauthorized access, modification, disclosure, or destruction.
    - Report Violations - All Mediware employees, contractors, and sub-contractors are required to report any known or suspected violations and/or security concerns to management, Information Security, or the HIPAA Privacy Officer. All Mediware employees, contractors, and sub-contractors are required to report faulty physical controls/equipment (shredders, door locks, etc.) as well.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Data is encrypted in transport using a third-party SSL/TLS certificate, employing 2048-bit keys for digital signatures, and Counter with Cipher block chaining mode (CCM), with AES-256 for message authentication and a SHA2-256-bit hash for secure hashing.

Data is encrypted at rest on disk for both OLTP databases and database backups using AES-256-bit encryption.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Mediware agrees to report to the customer under the Master Agreement any use or disclosure of the Protected Health Information not provided for by the BAA of which it becomes aware.

Mediware shall notify the customer of a breach of the Privacy Rule relating to the impermissible use or disclosure of Protected Health Information provided to the Mediware for purposes of carrying out its obligations under the Agreement. Unless otherwise required by law or agreed to by the parties, it shall be the responsibility of the customer to communicate with affected individual(s), the Secretary of HHS and the media information regarding the unintended use or disclosure.

Mediware's notification procedures are detailed in its Security Incidents and Breach Procedures, included with this proposal as Appendix A.

8.7 (E) Migration and Redeployment Plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Mediware's solutions are all commercial off the shelf software, configured per individual customers' requirements, and are licensed on a subscription basis, not sold. The proposal includes a Software as a Service (SaaS) delivery model, which relieves customers of the need to manage hardware, software, security, network and other aspects of the Mediware hosting infrastructure. As part of this SaaS model, Customers retain rights to their data, but retain no rights to continue use of said solutions following termination of the underlying Agreements. As such, Mediware has proposed a process for transition of customer data as part of a termination process, as applicable. Unless

otherwise specified in the applicable SOW, Order Form, or other contractual document, all work product developed, conceived, introduced, and/or delivered by Mediware in the course of performing services are owned by Mediware.

No later than six months prior to the termination of the contract, Mediware will provide a Transition Plan to assist customers in preparing for a transition to a new vendor solution per the process defined below.

When a customer decides to discontinue their service with Mediware, the customer is entitled to be provided with their data. In summary, Mediware prepare a set of files containing customer data using a standard process and make these files available to the customer for secure download.

The data includes

- All the customer data from all Mediware modules and Documents attachments databases; and
- *Harmony Advanced Reporting* database, if applicable.

Mediware responsibilities:

1. Disable access to all Mediware applications when advised
2. Establish accounts and assure access to the Mediware SFTP/FTPS site
3. Prepare customer data files and passwords
4. Provide data dictionary
5. Make files available for download on SFTP/FTPS
6. Provide one overview meeting of not more than two hours explaining files to the customer staff.
7. Provide:
    a. an initial set of files for testing and
    b. the final set of files after production data in Mediware systems has stopped.

All of the above files including the data dictionary are compressed, and encrypted (AES 256), and password protected using 7-ZIP and placed in a single 7-ZIP archive. This file is made available for download on the Mediware SFTP site using an SFTP account created for a singled designated point of contact. Mediware reserves the right to change the formats as we update our technology platforms and would advise the Agency of any such format changes as necessary

The above files contain the customer data only and will not contain:

- the existing Mediware schema;
- keys and constraints,

- stored procedures
- triggers; or
- any other non-data element/property/component/code that is proprietary to the Mediware solution.

Customer responsibilities

1. Disable end user access to all Mediware applications using the Mediware Customer Portal
2. Provide a single point of contact for accessing files via
3. Assure infrastructure in place to enable download and storage of files
4. Communicate shutoff date for data entry in production system
5. Download and test files provided by Mediware
6. Validate files by comparing on premise files to production database via the existing interfaces in the Mediware solution or via *Harmony Advanced Reporting*. Mediware will not provide any special validation scripts, or access method for this purpose
7. Coordinate with new vendor as needed for data mapping, conversion, migration to non-Mediware system

Any tasks, milestones or other transition tasks or services, consultation that are not detailed under “Mediware Responsibilities” above will be on time and materials contract and are not scoped as part of this proposal.

New Vendor Responsibilities

1. All other data mapping, conversion, migration analysis and tasks related to transition to the new vendor.

Steps/Milestones

We use the following process to create and deliver their data:

1. Customer: Establish single point of contact for SFTP/FTPS
2. Customer: Establish cutoff data for live data entry and communicate to end users
3. Customer: Provide written authorization to appoint individual(s) for SFTP access and enable Mediware to prepare and place files on SFTP/FTPS
4. Mediware: Prepare SFTP/FTPS site and accounts for the customer
5. Mediware: Authorized personnel is provided with credentials to access SFTP and password for file encryption
6. Mediware: Prepare batch one of files before cutoff of live data
8. Mediware: Prepare customer data files
9. Mediware: Make batch 1 files available for download on SFTP/FTPS
10. Customer: Download/test batch one of files before cutoff of live data

11. Customer: Disable end user access to all Mediware applications using the Harmony Customer Portal
12. Mediware: Prepare and make batch 2 (final batch) files available for download on SFTP/FTPS
13. Customer: Download batch 2 (final batch) of file after cutoff of live data

Contingency

If there is a failure to transition to a new vendor, Mediware will be pleased to discuss the process for re-enabling Mediware products with the customer and associated subscription fees.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

The orderly return of customer data is described in Section 8.7.1 above and is not repeated here for brevity.

8.8 (E) Service or Data Recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.
b. Suffers an unrecoverable loss of data.
c. Offeror experiences a system failure.
d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Mediware has a documented process for Priority 1 (P1) outages.

> *A P1 is defined as "A Critical business impact/service down: Business-critical Functionality is inoperable or critical interface has failed. This usually applies to a production environment and indicates an inability to access services resulting in a critical impact on operations."*

If the system or data is determined to be unrecoverable after 4 hours, a Disaster Recovery (DR) event is declared and the data center recovery plan is acted upon. This

is in parallel to other efforts that are working to restore normal business functions in the primary data center. Before the 4-hour time frame, a DR event can be declared by the Incident Manager. Mediware does not differentiate between various risk types or situations, all P1 outages are responded to in kind.

Mediware has provided a detailed discussion of its DR strategy in Section 8.15.3 and it is not repeated here for brevity.

8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

The process of backing up databases, system state, files, and other data refers to making periodic copies of critical data and storing this data on alternate media and locations. In the event of data loss these alternate data copies are used to restore systems to previous states. Mediware uses a combination of overlapping backup strategies that include SAN snapshots, backup snapshots, daily backups and incremental backups. Backup files created from these various backup processes are copied to various redundant storage devices as a staging point for the replication to DR site process. Backup files that contain PHI are encrypted before they are written to disk. All data is encrypted at rest using an approved FIPS 140-2 approved algorithm (AES-256). These files are backed-up to local storage. Data integrity and verification tests ensure that the data being backed-up is consistent and capable of being restored in the event of data loss. Data integrity test are performed during each backup job. Mediware restores a minimum of 100% of the production environment in monthly increments, at least once annually.

b. Method of server image backups

Using Veeam, Mediware provides fast, flexible and reliable recovery of fully virtualized VMs and data running on-premises or in our private cloud architecture. We backup application servers at least once a day, and backup SQL logs at least every 2 hours. Those backups are then sync'd to our DR datacenter in Kansas.

Mediware also utilizes native Nimble SAN to SAN image snapshot replication to replicate, near real time, to our DR center in Kansas.

c. Digital location of backup storage (secondary storage, tape, etc.)

Mediware utilizes enterprise grade, best in class storage devices including SAN and NAS devices from Nimble, Sonology and Verde. Both the SAN snapshots and Veeam backups are created locally at the IO Phoenix datacenter and replicated to our DR site at the TierPoint Kansas datacenter.

d. Alternate data center strategies for primary data centers within the continental United States.

Mediware utilizes 2 main datacenters.

IO Phoenix (Production)
615 N 48th St, Phoenix, AZ 85008

TierPoint Kansas (DR)
14500 W 105th St, Lenexa, KS 66215

8.9 (E) Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

In Mediware's SaaS solutions, data is encrypted in transport using a third-party SSL/TLS certificate, employing 2048-bit keys for digital signatures, and Counter with Cipher block chaining mode (CCM), with AES-256 for message authentication and a SHA2-256-bit hash for secure hashing.

Data is encrypted at rest on disk for both OLTP databases and database backups using AES-256-bit encryption.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Mediware is willing to sign a relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect customer data.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Mediware will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Mediware will not use customer data or customer-related data for any other purpose including but not limited to data mining, unless agreed by the customer through amendment of the Master Agreement, participating addendum, or related service level agreement. Mediware or its subcontractors will not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

8.10 (E) Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Mediware is willing to negotiate its SLA.

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Mediware has provided its Standard Service Level Agreement as an attachment to its submission (filename: "Mediware SLAs.pdf").

8.11 (E) Data Disposal

Specify your data disposal procedures and policies and destruction confirmation process.

All media containing customer data is destroyed securely by a NAID certified third party vendor pursuant to NIST Special Publication 800-88, Revision 1. As needed, Mediware provides a full accounting including a certification of secure destruction and a full inventory of the media destruction by serial number.

8.12 (E) Performance Measures and Reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Mediware complements a robust and highly available design with attentive monitoring and operational rigor. Mediware maintains the service levels of the SaaS environment by carefully managing the environment, and paying attention to security, network infrastructure, application response time and performance. Mediware uses tools that measure the availability and performance of the application. In addition, Mediware employs infrastructure monitoring tools that monitor the health of the underlying network and server infrastructure. Based on these metrics and resulting analysis, Mediware plans for capacity and expansion, and attempts to minimize the occurrence of incidents and/or down time. When incidents do occur, Mediware takes care to identify the root cause and put in place a remediation plan as necessary. Based on metrics collected from the monitoring tools, Mediware analyzes the results, and develops and implements plans for maintaining and improving service levels. Mediware uses these same results to proactively address capacity needs to assure that the application environment is in a continuously healthy state.

Capacity Management

Mediware monitors the workload on servers, disk, network, firewall, database servers and the other elements of the underlying infrastructure to assure that the application environment is sized properly and is tuned optimally to meet customer demand within existing service level agreements. Mediware regularly conducts estimates on server and network load and projections on disk storage growth for example to assure that the infrastructure is scaled well ahead of demand. As the SaaS solution environments expand, Mediware also makes resource decisions to support the environment as it grows in size and complexity. Mediware maintains healthy and manageable ratio of staff to infrastructure.

Service Continuity and Availability

The architecture has been designed to achieve a high degree of redundancy and availability. Each component part of the solution has redundancy, from the disk to the controller, and all the way to the network perimeter. The Mediware approach,

complemented by regimented backup procedures assures high levels of availability. Mediware regularly assesses continuity and availability risk in the design phase and revisits these issues at least quarterly through a review of the performance metrics and overall architecture and design. Mediware examines aspects including manageability of the infrastructure and application; reliability of the solution and underlying network and hardware; and current service contracts.

Mediware's track record on availability exceeds 99.5%. Mediware's standard availability SLA is 98%, but Mediware is willing to negotiate a higher standard up to 99.5% with Purchasing Entities as desired.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

As above, Mediware's track record on availability exceeds 99.5%. Mediware's standard availability SLA is 98%, but Mediware is willing to negotiate a higher standard up to 99.5% with Purchasing Entities as desired. Mediware has included its standard availability SLA as an attachment to its submission (filename: "Mediware SLAs.pdf").

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

Mediware has provided a detailed narrative regarding customer support in Section 8.4.2 and it is not repeated here for brevity.

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

Mediware has provided its standard support SLA as part of its standard master license and service agreement provided as an attachment to its submission (file name: "Mediware Master License Agmt.pdf"). It is not repeated here for brevity.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

Periodically, Mediware will schedule times when the system will be unavailable due to extended maintenance. If at all possible, these periods will be scheduled outside of normal business hours, and the subscriber will receive 24 hours' notice of the down time. Depending upon the immediacy of the maintenance required, the down time may

be rescheduled at the request of a subscriber. It is anticipated that there will be a weekly scheduled down time for system maintenance on Sunday evenings from 6:00 PM to 10:00 PM Eastern.

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

As outlined above, Mediware defines the overall service level of our Disaster Recovery service in the form of “Recovery Objectives.” These include:

- **Recovery Point Objective (RPO)** – Restoration point of database in event of disaster.
- **Recovery Time Objective (RTO)** – Time it takes to restore basic level of service after we officially declare a disaster.
- **Recovery Capacity Objective (RCO)** – The amount of capacity provided incrementally at various stages of the restoration process. Mediware capacity is measured in percentages of normal production capacity.

Mediware’s standard recovery objective targets are included below.

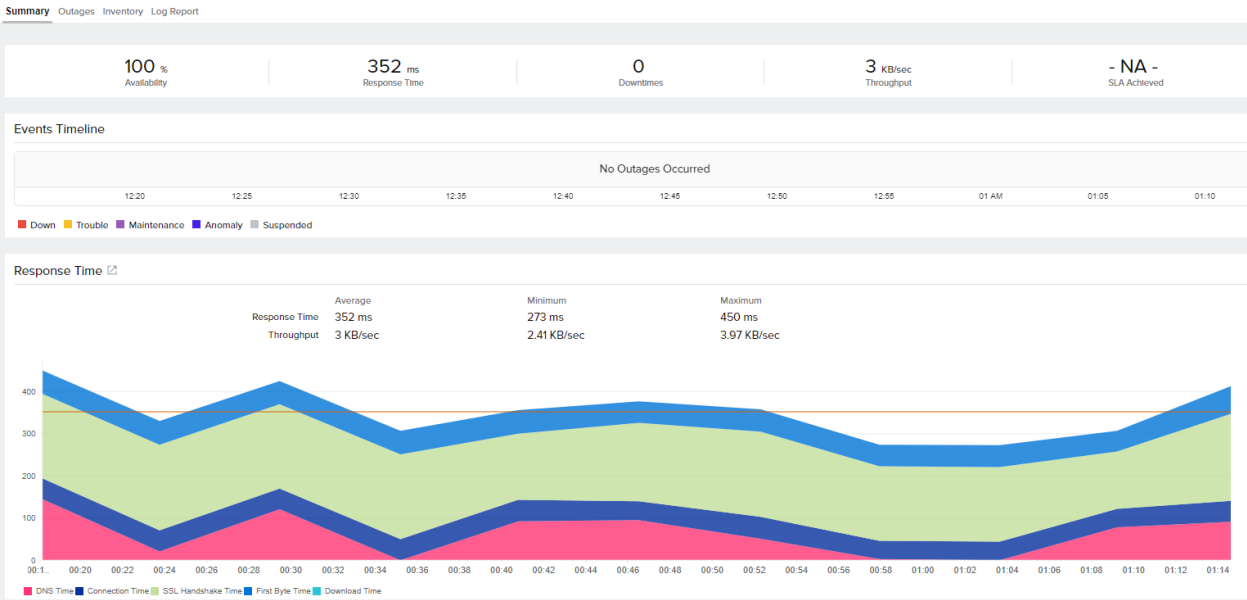
Recovery Objective	Target
RPO	48 hrs (Likely 24hrs.)
RCO/RTO	25% in 48 hours 50% in 96 hours 100% in 144 hours

Mediware’s standard SLA does not include explicit remedies for failure to meet these targets, but would be willing to discuss possible remedy language with participating entities during contract negotiation.

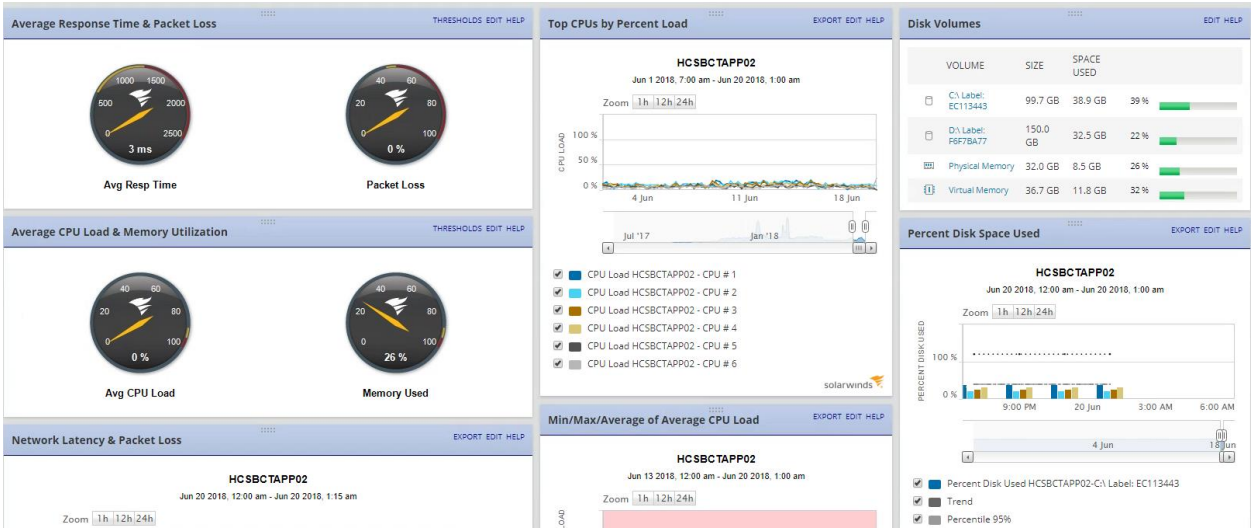
8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

Mediware uses several real-time enterprise tools to measure and report on the performance.

Example: Site 24x7 (available over the web)



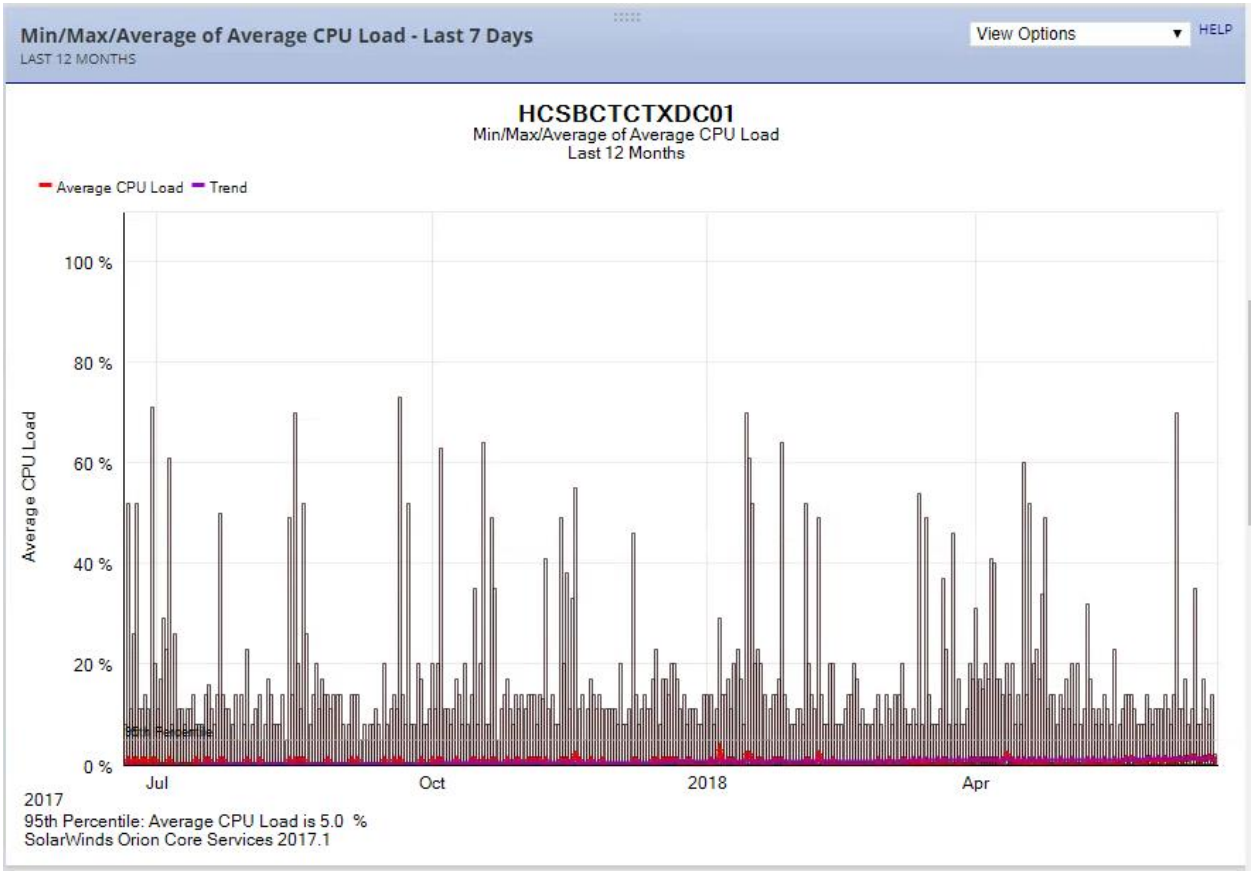
Example: Solarwinds



8.12.8 Ability to print historical, statistical, and usage reports locally.

Yes, Authorized users may access historical, statistical, and usage reports over the web to download and print.

Example: Site 24x7 (available over the web)



8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

Mediware's SaaS solutions are available 24/7/365, except for planned outages and maintenance windows.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Mediware has taken several steps and implemented several processes to ensure that the data we serve is protected, backed-up, archived (if needed) and destroyed when warranted.

- Mediware's private cloud is based around an enterprise reference architecture, that includes N+1 hardware and networking.
- Mediware has adopted a "belt-and-suspenders" model for data protection that included local SAN to SAN snapshots, offsite SAN to SAN replication, local backups to disk, offsite replication of the backups and offsite backup to tapes for long term archival.
- All backups at rest, and in transit are protected via FIPS 140-2 encryption standards.

Mediware's private cloud is both elastic and scalable both vertically (by adding more machines into the pool of resources) and horizontally (by being able to add CPU and RAM to existing clusters or just the virtual guests. This allows Mediware to scale up and scale down per environment. Mediware's SaaS solutions are available 24/365.

For any archival needs or data destruction needs, Mediware contracts with First Federal for long term tape retention and follows U.S. Depart of Defense wipe guidelines for any data destruction needs.

8.13 (E) Cloud Security Alliance

Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 **and** 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)

Mediware would be willing consider CSA Attestation, Certification or Assessment if awarded a contract via the Purchasing Entity.

Mediware has completed Exhibit 1 to Attachment B, which is included with its submission (filename: "Mediware CAIQ Exhibit 1 to Attachment B.xlsx").

8.14 (E) Service Provisioning

8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Mediware's products are complex enterprise systems used by human services agencies to track and manage the services they pay for and deliver to consumers. It would be extremely unlikely that an agency would expect to implement a Mediware solution without significant advance planning or with the expectation of an immediate deployment. Mediware would process such a request and implement the desired solution as quickly as possible using its standard processes, though with additional oversight by management through the sales process and throughout the implementation and deployment. Mediware has substantial experience ramping up resources and finding efficiencies to accelerate sales, contracting, and implementation to meet customers' emerging priorities or to compensate for customer delays.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Typically, Mediware requires at least 2 weeks following contract execution to assign resources and begin implementation of its solutions. Implementations schedules depend on modules deployed and the complexity of the scope of services.

8.15 (E) Back Up and Disaster Plan

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Mediware has several solutions for short and long term legal retention provided by setting the retention of existing backup jobs, creating specific backup jobs for legal retention in addition to being able to write to tape and store backup data at offsite secure facilities.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Mediware recognizes that there are force majeure events and other unplanned events that Mediware has planned for and built our plans to mitigate for. The following is the list of events that our Disaster Recovery (DR) and Emergency Preparedness plans were designed around;

- Disastrous Fiber Cut
- Physical facility failure (network, cooling, power)
- Local catastrophe (plane crash, etc.)
- Pandemics

In the event of a disaster, Mediware has a DR plan that is acted on. This plan is tested annually, updated on a semi-annual basis and is audited against Mediware's Type 2 Soc 2.

Mediware's approach to emergency preparedness considers all of these impacts through the following general principles:

- Planning – Emergency preparedness is explicitly considered during operational decision making and strategic planning at a corporate level. Incidents are evaluated with an eye toward updating emergency procedures with "lessons learned."
- Redundancy – Essential services, equipment, and infrastructure are duplicated/mirrored, obtained from more than one vendor, and/or deployed in geographically separated locations.
- Documentation – Policies and procedures are documented and reviewed periodically to ensure accuracy and currency. Personnel are familiar with the documentation and know where to find it when needed.
- Training – Personnel engaged in customer operations are cross-trained in operational procedures. Personnel are also trained specifically in emergency response.
- Mobility/Portability – Mediware uses mobile workforce tools to enable access to its facilities, equipment, infrastructure, and emergency protocols from locations other than corporate offices.
- Practice and Validation—Mediware completes an annual disaster recovery exercise, and regularly scheduled business continuity exercises to test and validate our preparedness and response plan against several scenarios, including natural disaster, pandemic and other events. As part of these tests, we also complete regular recovery exercises, including restoration of customer data to our disaster recovery data center.

As noted in Section 6.1.A of this proposal, Mediware has an extensive plan for customers' business continuity during and after emergencies, including pandemic. Mediware also has corporate business continuity and emergency preparedness plans to ensure that its operations continue during and after an emergency affecting its facilities, infrastructure, or personnel.

The Mediware Disaster Recovery plan contemplates business continuity procedures and emergency preparedness and includes staffing at multiple locations throughout the continental United States. The alternate data processing facility (DR Data Center) is located in Lenexa, Kansas and disaster preparedness and technical procedures for customer data are documented below. The DR Data Center is located in Lenexa, Kansas and the nearby corporate home office is staffed with technical and administrative staff such that in the event of a regional pandemic affecting Phoenix, AZ, the infrastructure hosting operations can be maintained remotely by staff in Lenexa, Kansas or alternatively by staff in Reston, VA.

As part of the annual Mediware annual Disaster Recovery exercise conducted by an independent third-party, staff from both the Phoenix and Lenexa teams participates in the recovery exercise. Each team member is presented with:

- An overview of the Disaster Recovery Plan;
- A full copy of the Disaster Recovery Plan;
- Alternative processing procedures, recovery procedures and restoration procedure;
- Documentation of the infrastructure;
- Documentation of key vendor and supplier contacts; and
- Documentation of installation and recovery procedures;

This knowledge sharing enables the all participants to assure a smooth, secure transition of maintenance and operation for the hosting environment in the case of a disaster, pandemic or other event requiring business continuity procedures.

In summary, Mediware has the following in place:

- **A Plan**: A defined Disaster Recovery Plan and procedures for addressing various business continuity, and disaster scenarios, including pandemic. This plan includes communication procedures, technical recovery procedures, staffing, vendor involvement, and criteria consider customer and business priority, and invoke alternate processing or staffing as necessary.

- **People:** Key, cross trained staff at multiple locations across the US that are involved in the annual Disaster Recovery and Business Continuity exercises;
- **Process:** A process for knowledge transfer, training, refinement and practice of business continuity and disaster recovery procedures. This includes training and sessions to review new deployments and infrastructure as needed.
- **Technology:** including:
  - **Alternate processing facilities**
  - **Site to site date replication** including all the technical measures described in the Disaster Recovery section

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Overview: Business Continuity & Disaster Recovery

Mediware's solution architecture has been designed to achieve a high degree of redundancy and availability. Mediware complements a robust and highly available design with attentive monitoring and operational rigor, resulting in our track record of success. Mediware's design and regimented backup procedures are important aspects of the resilience of our SaaS infrastructure. The Mediware SaaS operation is a is supported by a dedicated team, monitoring the infrastructure events and end user experience performance on 24x7x365 basis.

Mediware endeavors to assure continue preparedness for contingency operations by regularly assessing operational continuity and availability risk in the design phase. Mediware revisits overall architecture and design at least quarterly through a review of performance metrics. Mediware examines aspects including manageability of the infrastructure and application, reliability of the solution and underlying network and hardware and our service contracts.

The Mediware contingency plan involves the following key components:

- **Routine Business Impact Analysis (BIA):** This exercise inventories all critical components of the SaaS operation and results in a prioritization of risk to the SaaS operation. Mediware also conducts a BIA for corporate systems including customer service, finance, human resources, and corporate email.
- **Two Site Data Center Design for Disaster Recovery (DR)**, designed for recovery in the event of a disaster affecting the production data center

- **Backups stored locally and replicated.** Backups are stored locally in the production data center, and replicated nightly to our DR data center.
- **A Contingency/Continuity Of Operations Plan (COOP**) that enables Mediware workers to work remotely or in alternate offices in the case of damage affecting the Reston or Essex Junction Mediware offices.
- **Designation of key personnel** assigned to DR procedures with routine updating of contact lists.
- **Collection of key vendor and supplier and contract information** in case needed in to support recovery efforts.
- **Detailed technical recovery strategies**, disaster declaration procedures outlined in the Mediware SaaS DR plan.
- **Annual DR tabletop exercise conducted** for the Mediware SaaS operation by an independent third party specializing in business continuity and disaster recovery.

The backup and replication process is as follows:

- Nightly differential and weekly full backups are stored to disk in production (IO-Phoenix).
- Each night, these disk backups are replicated to the TierPoint Kansas Datacenter infrastructure.
- In addition to daily backups, Mediware creates daily snapshots on its SAN infrastructure, and then replicates those snapshots to the TierPoint Kansas Datacenter infrastructure.

Mediware Backups

Mediware provides regular automated backups as part of the standard SaaS offering. The service is a combination of automated disk and tape backup for SQL database (customer data), system configuration, and the Mediware application. Each night, automated backups of all customer data are encrypted, saved to disk and backed up onto removable tape media, and replicated to our secondary data center in Lenexa, Kansas.

The backup and replication process is as follows:

- Nightly differential and weekly full backups are stored to disk in production (WHS).
- Each night, these disk backups are replicated to TierPoint (the secondary data center) via backup infrastructure.
- Archival tapes are used for a duplicate copy of all backups and rotated to a secure off-site First Federal storage facility weekly.
- Mediware maintains tape hardware in both data centers to assure we can restore archival tapes as well as near terms disk backups.

- In compliance with HIPAA standards, the end-of-year tape is stored for 7 years.
- Mediware tests backup and restores as part of our normal hosting operations and successfully backs up and successfully restores over 30 databases each night on a scheduled basis.

Mediware Data Center Locations

Mediware's Disaster Recovery (DR) approach employs a two data center strategy. The physical location and description of the location of Mediware hosting infrastructure is indicated below:

Location Name	Description	Link to Data Center Specifications
Production Data Center	IO Phoenix 615 N 48th St, Phoenix, AZ 85008	https://www.io.com/data-centers/phoenix-data-center/
Disaster Recovery Data Center	TierPoint-Kansas 14500 W 105th St Lenexa, KS 66215	https://www.tierpoint.com/data-centers/kansas/kansas-city-lenexa/

CoSentry (now TierPoint, KS) serves as failover site in the event of disaster at the Mediware contracted IO primary hosting facility, in Phoenix, AZ. This Disaster Recovery (DR) site is on standby in case a catastrophic event occurred that rendered the IO hosting facility inaccessible or unusable. The architecture of the Mediware maintains non-production hardware and virtual infrastructure at the secondary facility. These environments are on standby and in the case of a disaster, are repurposed as production environments.

- **Mediware has provisioned an MPLS circuit for connectivity between data centers**, enabling site to site replication of domain information and backups;
- **Active Directory replication:** Domain information is replicated between the primary and secondary data centers.
- **Mediware web/application servers are on standby** at the non-production data center. Each time a new production application deployment takes place, Mediware updates the DR environment web servers to match the production version. The intent is to maintain the same version of application code/build deployed in both the DR and production environments.
- **Mediware database (DB) servers are on standby** at the non-production data, ready to receive database restoration from the replicated backups of production data.

In the event of a catastrophic disaster at the production data center, Mediware confirms domain replication status of Active Directory. Existing capacity at the secondary site is used for initial application installation and restoration of the most recent database backups. Additional capacity is then provisioned. Once the initial footprint is operational, Mediware initiates a DNS change to redirect the production application URL to the new production instance of the application running at the secondary data center. Until full DNS propagation is complete, Mediware provides the customer with a direct interim IP address. Incremental capacity is provisioned until either:

- we reach full production capacity,
- we roll back to the original production data center, or
- a replacement footprint is established at another location

Mediware modifies its disaster recovery process as the state of technology, industry best practices and operational needs change.

Mediware Disaster Recovery Details

Disaster Declaration

- At the 16-hour mark after a continuous unanticipated interruption (system downtime), Mediware Executive Management (Recovery Management Team) will decide whether or not the recovery plan will need to be activated. Mediware decision will be affected by the nature of the interruption, the conditions in the market and the potential financial and/or operational impacts to the company created by the interruption and the relative difficulties in activating the recovery versus waiting for resolution.
- Designated customer personnel will be notified via email and phone calls as necessary.

DB Backups & Install Packages Shipped

- Mediware shall confirm the last known good offsite backup before the disaster event occurred and confirm the most recent date/time stamp of the backup.
- The production application installation packages and associated versions will be confirmed and be shipped if needed to the secondary data center. Mediware maintains the installation and code base in two locations; however, Mediware step is a precautionary measure.

Provision Hardware and Environment

- Mediware maintains a development/test environment in the secondary Data Center at the TierPoint location which will be repurposed to meet production needs. This is simply a matter of provisioning virtual web and SharePoint servers on Mediware owned private cloud infrastructure.
- As necessary, Mediware will supplement existing capacity until full production capacity is reached.

Install Applications and Restore Databases

- Mediware shall install the Mediware application to the current production build.
- Mediware shall confirm the application installation and configuration.
- Mediware shall restore the last known good full database backups to hardware in the TierPoint Data Center. As necessary and applicable, Mediware shall restore the recent transactions logs/ differential backups to restore to the most recent known point in time of the data (before disaster).
- Mediware and Customers coordinate on reconfiguration of integrations that are dependent on Customer hosted infrastructure/services. An example would be an interface between Mediware and Customer systems.

Install Applications and Restore Databases

- Mediware shall perform initial validation to confirm environment at DR location is functional, including confirmation of functionality and Recovery Point Objective.
- Mediware to redirect DNS of Site URLS and Integration URLs, other dependencies.
- Mediware shall advise customer of alternate access methods as necessary, including direct URL.
- Accordingly, customer to release to user community when customer staff validation has been completed.
- As necessary, joint customer/Mediware planning to inform user community when full capacity in the DR location will be available.
- As necessary/appropriate, joint customer/Mediware planning to monitor and advise of rollback to primary data center pending restoration of services/repair and confirmation of same.

Mediware defines the overall service level of our Disaster Recovery service in the form of “Recovery Objectives”. These include:

- **Recovery Point Objective (RPO)** – Restoration point of database in event of disaster.
- **Recovery Time Objective (RTO)** – Time it takes to restore basic level of service after we officially declare a disaster.
- **Recovery Capacity Objective (RCO)** – The amount of capacity provided incrementally at various stages of the restoration process. Mediware capacity is measured in percentages of normal production capacity.

Mediware's standard recovery objective targets are included in Mediware proposal and listed below.

Recovery Objective	Target
RPO	48 hrs (Likely 24hrs.)
RCO/RTO	25% in 48 hours 50% in 96 hours 100% in 144hours

8.16 (E) Hosting and Provisioning

8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Mediware uses standard build processes derived from documented processes, checklists and templates. All provisioning activities and duties, in addition to other changes follow Mediware's Change Control process.

Change Management

Overview

In order to maintain a reliable and stable environment the Cloud Hosting Services Team (CHST) follows basic change management processes. This section describes the overall methodology and process used when making changes in the Cloud Hosting Services environment.

Planning

When it is determined that a change to the Cloud Hosting Services environment needs to be made, the CHST meets and discusses the plan to make the change. Elements of the plan include:

- Reason for the change
- Timing
- Cost
- Effected systems
- Is a downtime required? If so how long and what is the impact to clients
- Back-out Procedure
- Validation plan

Maintenance Windows

Regular maintenance is required to maintain system health and reliability. When possible, maintenance is performed in

A manner that does not require system downtime; however certain maintenance tasks require a system wide downtime. The CHST meets weekly to discuss needed updates and system changes that will be planned for the next maintenance window. The maintenance window will be no longer than four hours a month, unless a longer period is required. The regular maintenance window will be performed on the 3rd Wednesday of each month, unless notified at least two weeks in advance of the regularly scheduled maintenance window. When a longer downtime is required, the CHST will work with the Account Managers and clients to arrange a time that is least disruptive.

Downtime notifications are communicated with customers prior to the scheduled date. Notification is done via website, email, and voice when necessary.

Emergency Change

In the event an emergency change needs to be made e.g. a server reboot or an emergency patch, the CHST will notify Client Services, Professional Services and the management team with the expected impact and timing before any change is performed.

Staging

The process for a change (when applicable) should move through a test/dev/staging environment first then into production. When appropriate the CHST will notify clients that a change has been applied to their test environments and should be reviewed. The notification includes the date and time the change was applied and the anticipated date the change will be applied to production.

General Specification Updates

The General Specification is updated annually by the CHST and other departments. These updates are made available internally and to the client.

8.16.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

VMWare/vCenter/VCM

2. Creating and storing server images for future multiple deployments

VMWare/vCenter/VCM

3. Securing additional storage space

VMWare/vCenter/VCM, Nimble Storage

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

Solarwinds (SAM, IPAM, NPM, LEM), Site 24x7, AlertSite, SentryOne SQL Monitor and SumoLogic, Nimble/HPE Infosite.

8.17 (E) Trial and Testing Periods (Pre- and Post- Purchase)

8.17.1 Describe your testing and training periods that your offer for your service offerings.

System Testing

Testing of the entire system, end to end, helps ensure that the solution performs in accordance with the specifications and ratified configuration/design documents for the solution. Specific activities may include stress testing, volume testing and interface testing, depending on the scope of the deployment. Stress and volume tests would be iterative tests of performance under load with mutually agreed-upon performance targets and methodology. Integration testing is treated in the same manner as any other product provided by Mediware. Development and implementation yield analysis and design documentation that captures not only the functional requirements but also requirements around performance, volume, and proper error handling (including retry logic where applicable). The testing phase takes all of this into consideration before the

integration is considered production ready. Mediware has extensive experience building integration touch points and is well suited for handling implementations from file import/exports to Web Service interfaces.

A formal “go / no-go” decision is made at the conclusion of each of the planned Solution Acceptance Tests to determine whether the project is sufficiently meeting requirements to enable continued progress. The decision will be made jointly by Mediware and the customer on the basis of acceptance criteria previously defined in each of the component testing plans. In addition, Mediware submits a Solution Acceptance Test Result document for customer review and approval within ten (10) business days after test completion.

Mediware submits a User Acceptance test scripts and test plan during the validation phase of the project. The customer is responsible for conducting the tests on an agreed timetable.

User Acceptance Testing
The User Acceptance Testing (UAT) is facilitated by the customer project team with the assistance of the Mediware project team. Test cases and scripts are prepared by Mediware and the team from the customer. UAT is the first opportunity for the customer do a hands-on validation of the system’s configuration through the entire business process. The parties will work collaboratively through the validation. The formal UAT period is limited in duration as defined in the Test Plan and the comprehensive project schedule. Mediware will identify and designate a schedule and protocol for the reporting and remediation of identified defects in the Solution, so as to capitalize on the testing expertise and development / configuration resources for effective resolution. As defined in the testing procedures and documented in the appropriate test plans, Mediware and the customer agree on the severity rating of identified issues and the appropriate resolution plan for such issues.

The Project Team provides for UAT the test scripts defining the tasks to be performed and the expected result of performing each task. The specific tasks and functions to be performed will be stated in the UAT scripts, as defined during requirements gathering. The customer is responsible for providing business case scenarios to illustrate the user – defined tasks and steps.

The customer project manager works with the Mediware project manager to develop a testing plan that addresses topics such as validation objectives, customer resource assignments, validation instructions, testing activity agenda, testing schedule, validation results reporting, and validation acceptance criteria all based on the scope of services.

The overall objectives of validation are to test the customer process workflow as documented during requirements mapping. Testing activities may also include use case scenarios based on user roles, tasks and processes, and manual entry of representative data for report testing.

Customer testers document validation findings and communicate results to the project team. Validation findings may include variances between requirements documentation and configuration setup as well as gaps between the Mediware solution workflow and customer user expectations or preferences. The project team will review and assess validation findings and agree upon a resolution response to all items.

Integration testing is performed iteratively during the configuration phase to validate that each interface behaves as described in the interface design document, including accurate data transfer and exception handling. When User Acceptance Testing begins, any real-time, on-demand interfaces would be included in those tests to simulate actual workflow.

Upon acceptance of the validation results, the project will move into the training phase.

Training

Mediware typically follows a “Train-the-Trainer” approach as part of most implementation projects. During the early phases of the project, Mediware works with the customer’s Training Lead to plan the details of the training plan to work within the overall scope and timeline of the project. Once trained, the customer’s Trainers will complete all required end-user training with the direct guidance and supervision of Mediware’s implementation consultants.

Mediware’s training approach is based on best practices for adult learners. However, knowing that each project is also unique, Mediware’s implementation consultants will perform a discovery and needs analysis during the planning phase of the project to ensure the scope as outlined in the statement of work will meet the customer’s needs with respect to:

- The key roles to be trained
- The general technical proficiency of the stakeholders in those roles
- The knowledge required to ensure role-based proficiency with the new system
- Locations for training

From Mediware’s perspective, training is more than providing instruction on which buttons to push and when; it is an interactive process that can make or break system adoption. Mediware’s approach to curriculum involves a role-based instructional design philosophy that users need training based upon the specific features or functions related

to their work role(s). Mediware's "standard" curriculum reflects the practical application of role-based expertise developed over years of assessing what worked well in previous implementations, with updates to reflect customer-specific workflows. Mediware takes a systemic approach for measuring and managing training quality and effectiveness across the entire Training Phase. Post-training debriefs and surveys, and anecdotal insight from informal discussions are used to measure, control, and manage training quality. Mediware uses this feedback to actively enhance its training on a continual basis.

8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

In addition to the fully configured system provided for User Acceptance Testing as described above in Section 8.18.1, Mediware can also work with customers to provide a pilot phase for the solution delivered to a subset of users. Mediware has experience assisting customers to designing pilots and defining evaluation criteria to support the decision to expand the deployment to the larger group of users.

8.17.3 Offeror must describe what training and support it provides at no additional cost.

The solution support described in Section 8.4.2 is included in the annual SaaS subscription to Mediware's application modules. The training described in Section 8.17.1 is proposed per implementation, based on the scope and complexity of the project and the modules to be deployed. Training is included in any implementation fees proposed for the specific deployment.

Mediware also provides a limited of web-based on-demand training materials for some Mediware products. Access to these training products is included with SaaS subscription to the applicable modules.

8.18 (E) Integration and Customization

8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Mediware's SaaS Cloud Services provide rich interface capabilities that can support a broad range of system integration options for both large batch data exchanges and small, lightweight transactional data exchanges. Typically, Mediware utilizes Secure FTP (batch file transfer), FTPS (batch file transfer) or HTTPS (web services) options for data transport, and HIPAA Compliant EDI, XML, JSON or character delimited files (e.g., .CSV) data formats.

8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Most of Mediware's SaaS solution modules include built-in configuration utilities that allow customers to customize and personalize the business rules, workflow, security permissions, available data, screen appearance and content. Two of our primary SaaS solutions include a built-in Screen Design utility, which allows an agency to define an unlimited number of assessments or forms for data entry with dozens of different field types (e.g., lookup, text, date, checkbox, etc.) through configuration of the existing software, rather than through custom development by Mediware or through the use of external development toolboxes. This speeds implementation and reduces risk. Configuration tools also allow extensive configuration of core screens, including showing, hiding, re-ordering, and re-labeling fields to match agency terminology and role-based workflow. During implementation, Mediware configures the system to match customer requirements and trains System Administrators to use these built-in tools to update and maintain the system as needed if requirements change. This allows customers to make needed changes without engaging a vendor to make costly updates to the system when the agency needs to change the way it collects data to meet state and federal requirements.

These solutions also include the ability to alter or create new output document templates, whether through MS Word merge documents that draw information from the system to populate form letters or customized report formats developed through *Harmony Advanced Reporting,* Mediware's business intelligence and ad hoc reporting module. During configuration, Mediware configures and deploys MS Word document templates or, when necessary, reports in *Harmony Advanced Reporting*, to meet customer requirements for letters or other output documents. Templates are made

available in workflows and in selected areas of the solution to enable automated generation and attachment to appropriate records.

8.19 (E) Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

It will be in Mediware's best interest to actively promote the rigorous standards met as part of the NASPO ValuePoint Master Agreement, as well as the advantages of this program to procurement officials. Here's how Mediware will do it:

Multi-Pronged Marketing

Mediware will actively promote its NASPO ValuePoint Master Agreement via a multi-prong messaging approach that includes:

- **Nationwide technology events.** Mediware maintains a considerable presence at events for state technology leaders in the human services field. These include trade shows, symposiums, and invitation-only conferences. Before each event a planning meeting is held, where we will ensure the valued relationship with NASPO is part of the talking points, video displays, banners and collateral featured at these events.
- **Face-to-face meetings.** Mediware is recognized as the most experienced vendor in the human services space. We are frequently asked to share expertise and ideas, which will lead to many opportunities to share the advantages of the NASPO Approved Vendor Program.
- **Webinars.** Mediware regularly holds thought leadership webinars that include topics on the best ways to apply technology to the problems that states face. Mediware's relationship with NASPO will be mentioned during the standard "About Mediware" portion of these events.
- **Website promotion.** Mediware's new website coming in September includes strategic promotion of relationships like the NASPO Approved Vendor Program. More than a logo, the NASPO value proposition will be incorporated into appropriate sections of the site.
- **Sales collateral.** The NASPO relationship will be explained in collateral directed to state procurement officials.
- **Continual social media support.** Mediware's social properties will "follow" corresponding NASPO properties, which enables strategic mentions and re-posts of NASPO content.
- **Active communication with the public.** Mediware greatly values the work NASPO is doing to make state procurement more efficient. It will be in

Mediware's best interest to issue a press release on the NASPO relationship through PR channels, as well as pursue any available opportunity to inform the public on the critical issues affecting state procurement, and the work NASPO does on behalf of all citizens.

Targeted Messaging

Upon award of the contract, Mediware will conduct research to craft appropriate marketing messages to the various segments of eligible participants. The NASPO Master Agreement offers many advantages to state procurement officials. Messaging will be targeted to defined audiences based on:

- Procurement regulations in a given state
- Current relationship with Mediware
- Nature of the procurement

Mediware will then target each of the audiences we define, using the marketing channels listed above. Mediware will also leverage its exhaustive database of state technology buyers to target each audience via email and mail marketing. This will lead to broad-based awareness among each of these audiences, of the distinct advantages of procuring technology via the NASPO Master Agreement.

Customized Sales Process

Mediware will reinforce the value of the NASPO Master Agreement to participating procurement officials through a consultative, service-driven sales process.

- **Staff training and enablement.** All state-facing sales and technology staff will be trained on the advantages of the NASPO Approved Vendor Program, and how to convey that value to state agency contacts.
- **End-to-end communication support.** Sales collateral, informational literature and contractual documents used at every step of the sales process will describe and demonstrate the advantages of the NASPO Master Agreement.
- **Custom proposal process.** All proposals under this Master Agreement will comply with NASPO standards and will be written to clearly support those standards.

8.20 (E) Related Value-Added Services to Cloud Solutions

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Mediware provides a variety of professional services as part of implementation of its solutions. Mediware can also offer pre- and post-implementation value-added services as part of a contract or a contract addendum.

Implementation Services:

Mediware's implementation services for its SaaS product modules include the following professional and technical services. All of these services are not necessarily needed for each product module or in every solution deployment. As part of contract negotiation, Mediware proposes a statement of work outlining all recommended services to deploy customers' SaaS Cloud Solutions.

- Project management
- Project planning
- Requirements definition
- Requirements mapping
- Configuration
- Interface design
- Interface development/configuration
- Interface testing
- Interface deployment
- Data migration
- Solution validation
- User acceptance testing
- Training design and consultation
- Training (either train-the-trainer or end-user training; either on-site, remote, or self-led)
- Custom documentation
- Custom report development
- Pilot deployment
- Deployment/roll-out
- Go-live support

Once deployed, Mediware provides ongoing technical and product support, including maintenance of any custom interfaces, as well as product updates as they are released.

Pre-Implementation Services

Mediware offers professional and technical services to assist customer organizations to prepare for solution purchase. These services would be customer- and solution-specific and would be proposed in a defined scope of work prior to beginning work. These services may include:

- Business process consulting
- Requirements Definition
- Security Consultation
- Technical/Infrastructure Consultation
- Other professional or technical consulting

Post-Implementation Services

In addition to product and technical support provide as part of a customer's SaaS subscription, Mediware offers professional and technical services to update, maintain, and/or enhance their deployed solutions. These services would be customer- and solution-specific and would be proposed in a defined scope of work prior to beginning work. These services may include:

- Post-implementation audit services
- Training design and consultation
- Training (either train-the-trainer or end-user training; either on-site, remote, or self-led)
- Custom documentation
- Custom report development
- Data clean-up
- Interface design
- Interface development/configuration
- Interface testing
- Interface deployment

Mediware also offers standard services packages for new and existing customers to address resource shortages or improve performance, assist with enablement of new features during upgrades, and maximize value of the deployed solution. Mediware's services packages also include System Administration Services as a cost-effective method to handle ongoing system needs rather than staffing this function internally and/or back-filling departing system administration resources.

The three standard packages include:

- **Managed Upgrade Services** - to upgrade an existing implementation of the SaaS Cloud Services, validate fixes and review product enhancements for business workflow consideration.
- **Annual Wellness Checks** – to evaluate the level of satisfaction with a customer system's setups, processes, workflows, reports and other outputs and provide a report summarizing finding and recommendation to address any issues or opportunities for improvement.
- **System Administration Services** - A-la-carte model allows customers flexibility in number of monthly hours and choice in which administration tasks Mediware is responsible for, such as: General consultation, User provisioning, password resets, triaging application issues or configuration updates. System Administration Services also includes annual upgrades and wellness checks

Pricing and specific scope of these packages depend upon the customer's specific implementation.

8.22 (E) Supporting Infrastructure

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

Mediware's SaaS solutions are available over the Internet using only a web browser. Mediware makes recommendations to customers regarding bandwidth and connectivity to support satisfactory performance based on the number of users and anticipated business uses and workflows. Mediware recommends a minimum of 40 - 45 KBps for each concurrent user and a maximum latency 100ms or less round-trip end to end travel time from end user browser/computer to the Mediware SaaS site using the Mediware applications. Mediware does not support dial-up access.

Mediware also recommends workstation specifications and configuration per module. These recommendations are outlined in attachments included in Mediware's solution (filenames: "Harmony Computer Configuration Requirements - December 2017.pdf" and "Mediware Computer Configuration Requirements_2.1.pdf")

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Mediware's customers typically provide any required hardware, network infrastructure, browser, and operating software to use Mediware's SaaS solutions.

Appendix A: Security Incidents and Breach Procedures

On the pages following, Mediware is pleased to provide its standard operating procedure detailing its policy regarding security incidents and breach procedures. Page numbering is non-sequential.

Mediware®	**Security Incident and Breach Procedures**	
APPLICABILITY:	MEDIWARE INFORMATION SYSTEMS, INC.	DOCUMENT NUMBER: 16.1.5
COMPANY CONFIDENTIAL	QUALITY STANDARDS MANUAL	VERSION: 3
PAGE: 1 OF 17	MASTER / COPY:	EFFECTIVE DATE: 8/11/15

APPROVALS			
EX. VP, GENERAL COUNSEL R. WEBER SIGNATURE ON FILE	DATE 8/11/15	DIRECTOR, RA/QA J. MCGAHA	DATE 5/19/15
	DATE		DATE

REVISION HISTORY			
VERSION	SUMMARY OF CHANGES	AUTHOR	DATE
1	Initial release of document	J. Moeckel	2011
2	Change of document number from 15.0.3.7 to 15.0.2.5.	J. Moeckel	04/27/12
3	Document changes to reflect Omnibus Final Rule and organizational changes. Document name change from Incident Handling and Brach Analysis/Notification Procedure to Security Incident and Breach Procedure. Document number change from 15.0.2.5 to 15.1.5 and to 16.1.5	J. Moeckel	01/24/14

Mediware	Security Incident and Breach Procedures	
APPLICABILITY:	MEDIWARE INFORMATION SYSTEMS, INC.	DOCUMENT NUMBER: 16.1.5
COMPANY CONFIDENTIAL	QUALITY STANDARDS MANUAL	VERSION: 3
PAGE: 2 OF 17	MASTER / COPY:	EFFECTIVE DATE: 8/11/15

1.0 PRINCIPLE

1.1. 45 CFR 164.308(a) (6) (i) *Security Incident Procedures*: Implement policies and procedures to address security incidents.

1.2. 45 CFR 164.308(a)(6)(ii) *Response and Reporting* - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity and document security incidents and their outcomes.

1.3. 45 CFR § 164.410 *Notification by a Business Associate* - A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.

1.4. 45 CFR § 164.410 (a)(2) *Breaches treated as discovered* - For purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate.

1.5. 45 CFR § 164.410 (b) *Timeliness of Notification* – Except as provided in164.412, a business associate shall provide notification required by paragraph (a) of this section without reasonable delay and in no case later than 60 calendar days after discovery of a breach.

1.6. 45 CFR § 164.410 (c) *Content of Notification* – the notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach.

1.7. A business associate shall provide the covered entity with any other available information that the covered entity is require to include in notification to the individual under 164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.

2.0 SCOPE

2.1. This policy/procedure applies to all workforce members, departments, business units, and business partners of Mediware.

2.2. This policy/procedure applies to the following incidents:

2.2.1. Technical incidents (e.g., computer intrusions, denial of service to authorized users, etc.)

2.2.2. Non-technical incidents (e.g., administrative and physical incidents including but not limited to theft, unlocked doors, unauthorized facility entry, unauthorized computer access, etc.)

3.0 RESPONSIBILITIES

3.1. *Mediware Authorized User* – The Mediware Authorized User is responsible for reporting any suspected or actual security incident to the IT Department (Help Desk) or Privacy/Security Official.

3.1.1. Report the incident immediately.

3.1.2. Block or prevent incident escalation if possible.

3.2. *IT Department (Help Desk)*–IT Manger or designee is responsible for detecting, responding to and reporting all suspected or actual security incidents.

3.2.1. Escalate all incidents to the Privacy / Security Official.

3.2.2. Block or prevent incident escalation or further attack, if possible.

3.2.3. Repair the damage caused by the incident.

3.2.4. Preserve evidence of incident, when possible.

3.3. *Privacy/Security Official*: Is responsible for all investigation, mitigation, reporting, notification and documentation of all suspected or actual security incidents. The Privacy/Security Official is also responsible for breach determination and procedures.

4.0 REFERENCES

4.1. National Institutes of Standards and Technology: Computer Security Incident Handling Guide, NIST Special Publication 800-61.

5.0 RELATED DOCUMENTS

SOPP Number	Template, Form, or Guide	Title
16.1.2	SOPP	Information Security Policy and Procedures
16.1.3.3	SOPP	Device and Media Controls
16.1.4	SOPP	Facility, System and Information Access Management
16.1.5_F_1	Form	Incident Notification Form

SOPP Number	Template, Form, or Guide	Title
16.1.5_F_2	Form	Incident / Breach Report
16.1.5_F_3	Form	Breach Risk Assessment Tool
16.1.6	SOPP	Data Backup and Contingency Planning
17.4.34	SOPP	Contingency Operations
17.4.35	SOPP	Security Incident Procedures
17.4.36	SOPP	Response and Reporting

6.0 POLICY

6.1. Mediware will implement security incident and breach procedures to consistently detect, respond and report suspected or actual security incidents, to minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.

6.2. It is Mediware policy to safeguard the confidentiality, integrity and availability of PHI/ePHI, confidential and internal information through an established process. The process will address at a minimum:

6.2.1. Continuous monitoring of threats through reasonable and appropriate intrusion detection systems or monitoring practices.

6.2.2. Establishment of clear procedures for identifying, responding, assessing, analyzing and follow-up of incidents.

6.2.3. Workforce training, education and awareness on this policy and procedure.

6.2.4. Facilitation of clear communication of incidents with internal, as well as external stakeholders, if applicable.

6.2.5. *Security Incident* – Means the attempted or successful unauthorized access, use disclosure, modification or destruction of information or interference with Enterprise Information System operations.

6.2.5.1. Loss of asset or information through theft or loss, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

6.2.5.2. All security incidents have the potential for jeopardizing the confidentiality, integrity or availability of the information system or information being processed, stored or transmitted.

6.2.5.3. A security incident is a violation or imminent threat of a violation, of an explicit or implied security policy, acceptable use or standard practices. While certain adverse incidents, (floods, fires, etc.,) can cause system outages or damage, they are not considered security incidents.

6.2.5.4. A security incident becomes a breach, when the security incident involves the suspected or actual loss, access or disclosure of unsecured PHI/ePHI.

7.0 KEY CONCEPTS

7.1. *Event* - Is defined as an occurrence that does not constitute a serious adverse effect on the organization or its operations, though it may be less than optimal. Examples of events include, but are not limited to:

7.1.1. Hard drive malfunction that requires replacement.

7.1.2. Systems become unavailable due to power outage that is non-hostile in nature.

7.1.3. Accidental lockout of an account.

7.1.4. Network or system instability.

7.2. *Indication* – Is a sign that a security incident may have occurred or may be occurring at the present time. Examples of indications can be found in the attached Precursors and Indications, section 12.1 below.

7.3. *Precursor* – Is a sign that a security incident may occur in the future. Examples of precursors can be found in the attached Precursors and Indications, section 12.1 below.

7.4. *Security Incident* – Is an occurrence that exercises a significant adverse effect on people, process, technology, information or facilities. Security incidents are also violations or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to the following:

7.4.1. *Denial of Service* – An attack that prevents or impairs the authorized use of networks, systems or applications by exhausting resources.

7.4.2. *Malicious Code* – A virus, worm, Trojan horse, or other code-based malicious entity that infects a host.

7.4.3. *Unauthorized Access/System Handling* – A person gains logical or physical access without permission to a network, system, application, information or other resource. Hijacking occurs when an attacker takes control of network devices or workstations.

7.4.4. *Inappropriate Usage* – A person violates acceptable use policies, privacy and security policies and procedures or applicable Mediware policies and procedures.

7.4.5. *Unplanned Downtime* – The network, system, and/or applications are not accessible due to any unexplained circumstance causing downtime (e.g., system failure, utility failure, contingency operations, etc.).

7.4.6. *Multiple Components* – A single incident that encompasses two or more incidents (e.g., malicious code infection leads to unauthorized access to a host, which is then use to gain unauthorized access to additional hosts).

7.5. Mediware is aware that security incidents occur in countless ways. It is impractical to develop comprehensive step-by-step procedures for handling every security incident. Mediware will prepare as applicable to handle security incidents in accordance with regulatory standards and guidance from industry.

8.0 INCIDENT RESPONSE PLAN

8.1. *Alert / Identification Phase* – The alert / identification phase is the process of a Mediware workforce member or agent, learning about a potential event, indication, precursor or security incident and reporting it to the Help Desk or Privacy/Security Official. The Help Desk will immediately refer these to the Privacy/Security Official. Alerts may arrive from a variety of sources including, but not limited to:

8.1.1. System Users.

8.1.2. Monitoring activities.

8.1.3. Anti- virus software

8.1.4. Threats received via e-mail.

8.1.5. Media reports about new threats.

8.1.6. Individuals may use the following means to alert the Help Desk or Privacy/Security Official.

8.1.6.1. Email

8.1.6.2. Phone

8.1.6.3. Face to face

8.1.7. The Privacy/Security Official in collaboration with the IT Department will identify the situation as an event, indication, precursor or security incident and move into the triage phase.

8.2. *Triage Phase* –Involves the process of examining the information available about the situation to determine whether or not a security incident has occurred. If an event has occurred. The Help Desk will handle as appropriate or forward as necessary for resolution.

8.2.1. If an indication or precursor has been reported, the nature of the situation is determined, the initial priority level is assigned and the documentation of all action taken is initiated. A decision to pursue or protect is made during this phase according to the sensitivity of the data and criticality of the operational system.

8.2.2. If a decision to pursue is made, it assumes the situation continues as information about the malicious activity is being gathered. Before proceeding to protect, actions are initiated to discontinue the unauthorized actions as in the containment and eradication phases.

8.2.3. Protective actions will be performed on the system to safeguard data and system resources.

8.2.4. If the issue is a **security incident** the Privacy/Security Official activates the process and provides notification to Executive Management.

8.2.4.1. If a non-technical security incident is discovered. The Privacy/Security Official completes the investigation, implements preventative measures, completes documentation, provides report to Executive Management and resolves the security incident, as applicable.

8.2.4.2. If a technical security incident is discovered. The Privacy/Security Official in collaboration with the IT Department, begin response procedures.

8.3. RESPONSE (CONTAINMENT AND ERADICATION) PHASE(S)

8.3.1. The process of limiting the scope and magnitude of a security incident in order to keep the situation from getting worse and considered on the following factors such as system backup, the risk of continuing operations and changing passwords or access controls lists on the compromised systems and data. This also involves determining the cause of the security incident, improving system defenses, determining system vulnerabilities and removing the cause of the security incident to eliminate possibility of recurrence.

8.3.2. *Containment Phase (Technical)* – Mediware's IT Department attempts to contain the security incident. It is extremely important to take detailed notes during the security incident response process, including the use of appropriate procedures. This provides that the evidence gathered during the security incident can be used successfully during prosecution, if appropriate.

8.3.3. The IT Department along with the Privacy/Security Official review all collected information regarding the security incident.

8.3.4. The IT Department secures the physical and network perimeter.

8.3.5. The IT Department will perform the following, if applicable:

8.3.5.1. Load a trusted shell.

8.3.5.2. Retrieve all volatile data from the affected system.

8.3.5.3. Determine the relative integrity and appropriateness of backing the system up.

8.3.5.4. If appropriate, back up the system.

8.3.5.5. Change password(s) to the affected system(s), if appropriate.

8.3.5.6. Determine whether it is safe to continue operations with the affected system(s).

8.3.5.6.1. If it is safe, allow the system to continue to function. Complete any documentation relative to the security incident.

8.3.5.6.2. If it is unsafe to allow the system(s) to continue operation discontinue the system(s) operation and proceed to eradication.

8.3.5.6.3. The individual completing this phase provides communication as appropriate to the IT Manager and Privacy/Security Official.

8.4. *Eradication Phase (Technical)* – The Eradication Phase represents Mediware's effort to remove the cause, and the resulting security exposure, that are now on the affected system(s). The IT Department will:

8.4.1. Determine symptoms and cause related to the security incident.

8.4.2. Strengthen the defenses surrounding the affected system(s), where possible (a risk assessment may be needed). This may include the following:

8.4.2.1. An increase in network perimeter defenses.

8.4.2.2. An increase in system monitoring defenses.

8.4.2.3. Remediation of any security issues within the affected system(s), such as removing unused services/general host hardening techniques.

8.4.3. Conduct a vulnerability assessment to verify all identified holes/gaps that have been exploited, have been addressed, as appropriate. If additional issues or symptoms are identified, take appropriate preventive measure to eliminate or minimize potential future compromises.

8.4.4. Document the action taken during the Eradication Phase.

8.4.5. The individual completing this phase provides communication as appropriate to the IT Manager and Privacy/Security Official.

8.4.6. Upon successful completion of containment and eradication of the security incident, the process moves into the recovery phase.

8.5. *Recovery Phase*- The system and business process returns to full and normal operation during this phase. Actions include restoring and validating the system, deciding when to restore operations and monitoring systems to verify normal operations without further system or data compromise.

8.5.1. The IT Department will determine if the affected system(s) have been changed in any way.

8.5.1.1. If changed, the IT Department will restore the system to its proper, intended functioning.

8.5.1.2. Once restored, the IT Department will validate that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit or individual related to the security incident.

8.5.1.3. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor.

8.5.1.4. If the system(s) had not been changed in any way, but was taken offline, restart the system(s) and monitor for proper behavior.

8.5.1.5. Document the action and all applicable information regarding the recovery of the system(s).

8.5.1.6. The individual completing this phase provides communication as appropriate to the IT Manager and Privacy/Security Official.

8.6. *Follow-up Phase* – Involves developing the security incident report and disseminating it to appropriate entities according to established policies; identifying lessons learned from the incident, successful and unsuccessful actions taken in response, and developing recommendations to prevent future security incidents and improve security implementation. This phase is completed by the Privacy/Security Official with collaboration from the IT Department.

8.7. *Periodic Evaluation* – The security incident response will be periodically reviewed and evaluated for effectiveness and completeness. This also involves the appropriate training of Mediware's workforce, as well as resources expected to respond to security incidents.

8.8. *Documentation* – All documentation surrounding every security incident, to include all work papers, notes and other items relevant to the notification, investigation, report and notification of security incidents will be securely maintained and easily retrievable for a period of six (6) years.

8.8.1. The Privacy/Security Official will review and update documentation regarding the security incident response to ensure, at a minimum the following is documented:

8.8.1.1. Status of the incident

8.8.1.2. A summary of the incident (type of event, when it occurred, where it occurred, source of the event, and identityof any individuals or subject associated with event.)

8.8.1.3. Actions taken by all incident responders regarding the incident

8.8.1.4. A list of evidence gathered during the investigation

8.8.1.5. Comments from responders

8.8.1.6. Next steps to be taken (outcome of the event)

8.8.2. The Privacy/Security Official will be responsible for maintenance of the appropriate documentation.

9.0 BREACH POLICY AND PROCEDURE

9.1. Mediware's Privacy/Security Official will provide timely and appropriate notice within the extent required by law, when there is reasonable suspicion that a breach of PHI/ePHI has occurred.

9.2. *Disclosure* – Means the release, transfer, provision of, access to, or divulging in any manner of information outside of Mediware.

9.3. *Access* – Means the ability or the means necessary to read, write, modify, or communicate data / information or otherwise use any system resource.

9.4. *Breach* - Means the acquisition, access, use or disclosure of PHI/ePHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI/ePHI, is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI/ePHI has been compromised based on a risk assessment.

9.5. *Breach Excludes*

9.5.1. Any unintentional acquisition, access or use of PHI/ePHI by a workforce member or person acting under the authority of Mediware if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further acquisition, access or use, in a manner not permitted under the Privacy Rule.

9.5.2. Any inadvertent disclosure by a person who is authorized to access PHI/ePHI at Mediware to another person authorized to access PHI/ePHI at Mediware, or arrangement in which Mediware participates, and the information received as a result of such disclosure is not further disclosure in a manner not permitted under the Privacy Rule.

9.5.3. A disclosure of PHI/ePHI where Mediware has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonable have been able to retain such information.

9.6. *Unsecured Protected Health Information* – PHI/ePHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

9.6.1. Encryption as specified in the HIPAA Security Rule by the use of an algorithmic process to transform data into a form in which there is a low probability of

assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption, has not been breached. To avoid a breach of the confidential process or key, these decryption tools will be stored on a device or at a location separate from the information they are used to encrypt or decrypt. The following encryption processes meet the standard.

9.6.1.1. Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

9.6.1.2. Valid encryption processes for data in motion are those that comply, as appropriate, with NIST Special Publication 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS).

9.6.2. The media on which the PHI/ePHI is stored or recorded has been destroyed in the following ways:

9.6.2.1. Paper, film or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

9.6.2.2. PHI/ePHI, has been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the ePHI cannot be retrieved. Refer to 16.1.3.3 Device and Media Controls for further information.

9.7. *Discovery of Breach* – A breach of PHI/ePHI will be treated as "discovered" as of the first day on which a security incident that may have resulted in a breach is known, or by exercising reasonable diligence would have been known. Mediware will be deemed to have knowledge of a breach if such breach is known to any person, other than the person committing the breach, who is a workforce member or agent of Mediware.

9.7.1. Following alert of a security incident. The Privacy/Security Official will determine if a breach as defined by the regulations, has occurred. If it is determined that a breach has occurred. The Privacy/Security Official will start an investigation.

9.8. *Breach Investigation* – Mediware has designated the Privacy/Security Official to act as the investigator of the breach. The Privacy/Security Official will be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with individuals within Mediware, as appropriate.

9.8.1. The Privacy/Security Official will be the key facilitator for all breach notification processes to the applicable entities (e.g., customer, HHS, media, law enforcement officials, etc.).

9.8.2. All documentation related to the breach investigation, including the risk assessment and notification made, will be retained for a minimum of six (6) years.

9.9. *Risk Assessment* – For an acquisition, access, use or disclosure of PHI/ePHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI/ePHI that is permitted or otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. An "acquisition, access, use , or disclosure in a manner not permitted, is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment" of at least the following factors:

9.9.1. The nature and extent of the PHI/ePHI involved, including the types of identifiers and the likelihood of re-identification.

9.9.2. The unauthorized person who used the PHI/ePHI or to whom the disclosure was made.

9.9.3. Whether the PHI/ePHI was actually acquired or viewed.

9.9.4. The extent to which the risk to the PHI/ePHI has been mitigated.

9.9.5. The Privacy/Security Official will document the risk assessment as part of the investigation in the security incident report, noting the outcome of the risk assessment process. Mediware has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the Privacy/Security Official, following review from General Counsel, will move forward with breach notification. Mediware may make breach notifications without completing a risk assessment.

9.10. *Timeliness of Notification* – Upon determination that breach notification is required, the Privacy/Security Official, with approval by General Counsel, will make notice to the appropriate Covered Entity Customer, without unreasonable delay, in accordance with Business Associate Agreement, and in no case later than 60 calendar days after the discovery of the breach by Mediware or Business Associate involved that is acting as Mediware's agent. It is the responsibility of Mediware to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

9.11. *Delay of Notification* – Mediware may delay notification, if a law enforcement official determines that a notification, notice or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed.

9.11.1. If the statement is in writing and specifies the time for which a delay is required, Mediware will delay such notification, notice or posting of the time period specified by the official.

9.11.2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

9.12. *Contents of Notice* – Such notice will include the identification of each individual whose unsecured PHI/ePHI has been, or is reasonably believed by Mediware to have been, accessed, acquired or disclosed during such breach. Mediware will provide Covered Entity Customer with any other available information that the Covered Entity Customer is required to include in notification to the individual, or applicable entity, at the time of the notification or promptly thereafter as information becomes available. Unless required by law or agreed upon. The Covered Entity Customer will be responsible for notifying affected individuals and is responsible for breach reporting requirements to applicable entities (i.e., HHS, media). The Covered Entity Customer is responsible for the documentation of all notification or reporting requirements to individuals, HHS or the media.

9.13. *Methods of* Notification - The method of notification will depend on the Covered Entity Customer to be notified.

9.13.1. In each case, such notification shall be made only if required by law. The Privacy/Security Official will consult with General Counsel to develop the notification, determine the method of notification, if required, and make the final determination if notification is warranted.

9.14. *Maintenance of Breach Information/Log*: As described throughout the document and in addition to the reports created for each incident, Mediware will maintain a process to record or log all breaches of unsecured PHI/ePHI. The applicable information will be maintained by the Privacy/Security Official for a period no less than six (6) years and may contain, but is not limited to, the following:

9.14.1. A description of what happened, including the date of the breach, the date of the discovery and the number of individuals affected, if known.

9.14.2. A description of the types of unsecured PHI/ePHI that were involved in the breach.

9.14.3. A description of the action taken with regard to notification.

9.14.4. The results of the risk assessment.

9.14.5. Resolution steps taken to mitigate the breach and prevent future occurrences.

10.0 SANCTIONS

10.1. The Privacy/Security Official in consultation with General Counsel will make judgment regarding severity of the security incident or breach and appropriate disciplinary action up to and including termination of employment, contract or business arrangement. Appropriate legal action, including civil or criminal penalties, may be pursued depending on severity of security incident or breach.

11.0 ATTACHMENTS

11.1. Precursors and Indications (example)

PRECURSORS AND INDICATIONS

Denial of Service Precursors and Indications:

Malicious Action	Possible Indications
Network based DOS against a particular host.	▪ User reports of system unavailability ▪ Unexplained connection losses ▪ Network intrusion detection alerts ▪ Host intrusion detection alerts (until host is overwhelmed) ▪ Increased network bandwidth utilization ▪ Large number of connections to a single host ▪ Asymmetric network traffic pattern (large amount of traffic going to the host, little traffic coming from the host) ▪ Firewall and router entries ▪ Packets with unusual source addresses
Network based DOS against a network	▪ User reports of system and network unavailability ▪ Unexplained connection losses ▪ Network intrusion detection alerts ▪ Increased network bandwidth utilization ▪ Asymmetric network traffic pattern (large amount of traffic entering the network, little traffic leaving the network) ▪ Firewall and router log entries ▪ Packets with unusual source addresses ▪ Packets with nonexistent destination addresses
DOS against the operating system of a particular host	▪ User reports of system and application unavailability ▪ Network and host intrusion detection alerts ▪ Operating system log entries ▪ Packets with unusual source addresses
DOS against an application on a particular host	▪ User reports of application unavailability ▪ Network and host intrusion detection alerts ▪ Application log entries ▪ Packets with unusual source addresses

Malicious Code Attacks:

Malicious Action	Possible Indications
A virus that spreads through email infects a host	▪ Antivirus software alerts of infected files ▪ Sudden increase in the number of emails being sent and received ▪ Changes to templates for word processing documents, spreadsheets, etc.

	▪ Deleted, corrupted or inaccessible files ▪ Unusual items on the screen, such as odd messages and graphics ▪ Programs start slowly, run slowly or do not run at all ▪ System instability and crashes ▪ If the virus achieves root level access se Appendix B Unauthorized Access For Root Compromise Host.
A worm that spreads through a vulnerable service infects a host	▪ Antivirus software alerts of infected files ▪ Port scans and failed connection attempts targeted at the vulnerable service ▪ Increased network usage ▪ Programs start slowly, run slowly or do not run at all ▪ System instability and crashes ▪ If the virus achieves root level access see Unauthorized Access For Root Compromised Of Host
A Trojan horse is installed and running on a host	▪ Antivirus software alerts of Trojan horse versions of files ▪ Network intrusion detection alerts of Trojan horse client server communications ▪ Firewall and router log entries for Trojan horse client serve communications ▪ Network connections between the host and unknown remote systems ▪ Unusual and unexpected ports open ▪ Unknown processes running ▪ High amounts of network traffic generated by the host, particularly if directed at external host. ▪ Programs start slowly, run slowly or do not run at all ▪ System instability and crashes ▪ If the Trojan horse achieves root level access, see Unauthorized Access for Root Compromised Host.
Malicious mobile code on a web site is used to infect a host with a virus, worm or Trojan horse	▪ Indications listed above for the pertinent type of malicious code ▪ Unexpected dialog boxes, requesting permission to do something ▪ Unusual graphic, such as overlapping or overlaid message boxes
Malicious mobile code on a Web site exploits vulnerabilities on a host	▪ Unexpected dialog boxes, requesting permissions to do something ▪ Unusual graphics, such as overlapping or overlaid message boxes ▪ Sudden increase in the number of emails being sent and received ▪ Network connections between the host and unknown remote systems ▪ If the mobile code achieves root level access, See Unauthorized Access for Root Compromised Host.
User receives a virus hoax message	▪ Original source of the message is not an authoritative computer security group, but a government agency or an important official person ▪ No links to outside sources ▪ Tone and terminology attempt to invoke panic or sense of urgency ▪ Urges recipient to delete certain files and forward the message to others

Unauthorized Access Indications:

Malicious Action	Possible Indications
Root Compromise of a host	▪ Existence of unauthorized security related tools or exploits ▪ Unusual traffic to and from the host ▪ System configuration changes, including ▪ Process service modification or additions ▪ Unexpected open ports ▪ System status changes

	▪ Changes to log and audit policies and data ▪ Network interface card set to promiscuous mode ▪ New administrative level user account or group ▪ Modifications of critical files, timestamps and privileges; including executable programs, OS kernels, system libraries, configuration and data files ▪ Unexplained account usage ▪ Significant changes in expected resource usage ▪ User reports of system unavailability ▪ Network and host intrusion detection alerts ▪ New files or directories with unusual names ▪ Highly unusual operating system and application log messages ▪ Attacker contacts the organization to say that her or she has compromised a host
Unauthorized data modification	▪ Network intrusion detection alerts ▪ Increased resource utilization ▪ User reports of data modification ▪ Modification to critical files ▪ New files or directories with unusual names ▪ Significant changes in expected resource usage
Unauthorized usage of standard user account	▪ Access attempts to critical files ▪ Unexplained account usage ▪ Web proxy log entries showing the download of hacker tools
Physical intruder	▪ User reports of network or system unavailability ▪ System status changes (restarts, shutdowns) ▪ Hardware is completely or partially missing ▪ Unauthorized new hardware
Unauthorized data access	▪ Intrusion detection alerts of attempts to gain access to the data through FTP, HTTP and other protocols ▪ Host recorded access attempts to critical files

Inappropriate Usage Indications:

Inappropriate Action	Possible Indications
Unauthorized service usage	▪ Network intrusion detection alerts ▪ Unusual traffic to and from the host ▪ New process/software installed and running on a host ▪ New files or directories with unusual names ▪ Increased resource utilization ▪ User reports ▪ Application log entries
Access to inappropriate materials	▪ Network intrusion detection alerts ▪ User reports ▪ Application log entries ▪ Inappropriate files on workstations, servers or removable media
Attack against external party	▪ Network intrusion detection alerts ▪ Outside party reports ▪ Network, host and application log entries

Mediware®	**Security Incident and Breach Procedures**	
APPLICABILITY:	MEDIWARE INFORMATION SYSTEMS, INC.	DOCUMENT NUMBER: 16.1.5
COMPANY CONFIDENTIAL	QUALITY STANDARDS MANUAL	VERSION: 3
PAGE: 17 OF 17	MASTER / COPY:	EFFECTIVE DATE: 8/11/15

MEDIWARE HUMAN & SOCIAL SERVICES, INC.
MASTER LICENSE AND SERVICES AGREEMENT

This Master License and Services Agreement (the "Agreement") is entered into as of _____ (the "Effective Date"), by and between **Mediware Human & Social Services, Inc.,** with offices at 11711 West 79th Street, Lenexa, Kansas 66214 ("Mediware"), and _____, a _____ corporation with offices at _____ ("Customer"). Each of Mediware and Customer may be referred to herein individually as a "Party" and together as the "Parties." The Parties agree as follows:

1. **DEFINITIONS**. Capitalized terms used herein or in any Order Form, but not defined, have the meaning set forth in Exhibit A.

2. **LICENSED SOFTWARE**.

2.1. Licensed Software. Mediware grants to Customer (a) a non-exclusive, non-transferable, license to use the Licensed Software or (b) a limited term, non-exclusive, non-transferable, license to use the Licensed Software, subject to the terms of this Agreement and the applicable Order Form. Customer represents that it has authority to bind each Customer affiliate and Licensed User to the terms of this Agreement. Customer shall be responsible for all acts and omissions of all Customer affiliates and Licensed Users.

2.2. Limitations. No right to use, copy, modify, create derivative works of, adapt, distribute, disclose, decompile or reverse engineer the Licensed Software is granted, except as expressly set forth in this Agreement. Mediware reserves title to the Licensed Software and all rights not expressly granted hereunder. Customer may make copies of Licensed Software as necessary for back-up, testing and archival purposes only. Customer may not use any component of the System to provide services to third parties as a service bureau or data processor.

2.3. Scope of Use. The Licensed Software and Sublicensed Software are priced based on certain metrics (e.g. Sites, Deliverables and/or Licensed Users) as set forth in an Order Form. Customer may only expand its use of the Licensed Software or Sublicensed Software upon payment of additional license, support and service fees at Mediware's then-current rates. Any such fees for additional scope of use will be immediately due and payable.

3. **SERVICES.**

3.1. Cloud Services. During the Cloud Services term set forth in an Order Form, Mediware shall provide Customer a non-exclusive, non-assignable, limited license to access and use the Cloud Services, solely for Customer's internal business operations and subject to the terms of this Agreement and Order Form.

3.2. Support. Mediware shall provide the Support Services set forth in Exhibit B or in the applicable Order Form. For Cloud Services. Customer shall purchase any hardware and third-party software required to use the Licensed Software or Cloud Services. Mediware is not obligated to provide Support services for Licensed Software that is not the most current or next to most current release.

3.3. Professional Services. Unless otherwise set forth in an Order Form, Professional Services shall be performed on a time and materials basis at Mediware standard rates.

3.4. Customer Responsibilities. Customer shall approve access for all Licensed Users to the Cloud Services, and shall prevent unauthorized access and use of the Cloud Services. Customer shall not, and shall ensure that its Licensed Users do not: (i) sell, resell, lease, lend or otherwise make available the Cloud Services to a third party; (ii) modify, adapt, translate, or make derivative works of the Cloud Services; or (iii) sublicense or operate the Cloud Services for timesharing, outsourcing, or service bureau operations. For portal administration and user provisioning responsibilities, see the terms of Exhibit C.

3.5. Suspension of Services. If (i) there is a threat to the security of Mediware's systems or the Services, or (ii) Customer's undisputed invoices are 60 days or more overdue, in

addition to any other rights and remedies (including termination), Mediware may suspend the Services without liability until all issues are resolved.

4. **SUBLICENSED SOFTWARE AND HARDWARE**. Subject to the terms and conditions of this Agreement and any Order Form, Mediware shall grant the licenses to Sublicensed Software as set forth in an Order Form. Customer agrees to purchase any Hardware set forth in an Order Form.

5. **PROPRIETARY RIGHTS**.

5.1. Ownership. Mediware or its licensor retains all right, title, and interest, in the Licensed Software, Sublicensed Software, Test Scripts, Documentation, Services, and Work Product. Mediware shall grant to Customer a non-exclusive, non-transferable license to use Work Product only for Customer's own internal purposes in connection with the Licensed Software and Services.

5.2 Restricted Rights. The Licensed Software is commercial computer software programs developed exclusively at private expense. Use, duplication, and disclosure by civilian agencies of the U.S. Government shall be in accordance with FAR 52.227-19 (b). Use, duplication and disclosure by DOD agencies are subject solely to the terms of this Agreement, a standard software license agreement as stated in DFARS 227.7202.

6. **INSTALLATION OF DESIGNATED PLATFORM.** Customer shall install all components of the Designated Platform, and complete all necessary diagnostic tests to ensure such installation is complete and successful.

7. **PAYMENTS BY CUSTOMER**.

7.1. Payment. Customer shall pay all Fees for the Licensed Software, System Services and Hardware. All invoices shall be paid net 30 days following the date of the invoice. Invoices that are more than 10 days past due shall be subject to a finance charge at a rate of interest the lesser of 1.5% per month or maximum permissible legal rate.

7.2. Increase. All annual fees may be increased by Mediware once annually commencing one (1) year following the Effective Date of the applicable Order Form at a rate not to exceed 5%. Maintenance and Cloud Services fees may further be increased upon prior written notice to Customer in the event Mediware's third-party supplier increases such fees.

7.3. Expenses. Customer shall reimburse Mediware for all reasonable Customer-related travel, lodging and out-of-pocket expenses.

7.4. Shipping Fees, Taxes. Customer shall pay all shipping charges, as well as any taxes, fees or costs imposed by any governmental body arising as a result of this Agreement. Mediware shall be responsible for taxes on its net income.

7.5. Delivery/Risk of Loss. All materials provided by Mediware to Customer hereunder are shipped FOB Mediware's carrier.

7.6. Audit. Mediware reserves the right to audit Customer's use of the System and Cloud Services, remotely or on site at a mutually agreeable time. If Customer's use is greater than contracted, Customer shall be invoiced for any unlicensed use (and related support), and the unpaid license and support fees shall be payable in accordance with this Agreement. If any increase in fees is required, Customer shall also pay the expenses associated with the audit**.**

8. **LIMITED WARRANTIES AND COVENANTS**.

8.1. Licensed Software Warranty. Mediware warrants that the Licensed Software shall, without material error, perform the functions set forth in the Documentation when operated on the Designated Platform in accordance with this Agreement and the Order Form during the Warranty Period.

8.2. Services Warranty. Mediware warrants that it shall perform the Services in a professional manner in accordance with the applicable Documentation.

8.3. Hardware/Sublicensed Software. Customer agrees that the manufacturers or licensors of Hardware and Sublicensed Software may

provide certain warranties and other terms and conditions with respect to the Hardware and Sublicensed Software supplied to Customer under this Agreement. Mediware makes no representations or warranties concerning the Hardware or Sublicensed Software.

8.4. Remedy. Customer's sole and exclusive remedy for any breach of the warranties set forth herein or in an Order Form shall be to notify Mediware of the applicable non-conformity, in which case Mediware shall use commercially reasonable efforts to correct such non-conformity by redelivering the Licensed Software or re-performing the Services. Notwithstanding the foregoing, Mediware shall not be responsible for any non-conformity, which arises as a result of (i) any act or omission of Customer, including a failure to use the System or Cloud Services in conformance with the Documentation or Applicable Law; (ii) any person (other than Mediware) making modifications to the Designated Platform in any way without Mediware's prior written consent; or (ii) any failure of any component of Hardware, Sublicensed Software, or any Customer-supplied software, equipment or other third-party materials.

8.5. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN OR IN AN ORDER FORM, MEDIWARE DISCLAIMS, ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE AND MERCHANT-ABILITY, AND ANY WARRANTY OF NON-INFRINGEMENT, OR ANY WARRANTIES ARISING FROM TRADE PRACTICE OR COURSE OF DEALING. MEDIWARE DOES NOT WARRANT THAT THE SERVICES SHALL BE ERROR-FREE OR UNINTERRUPTED, OR THAT ALL DEFECTS SHALL BE CORRECTED, OR THAT THE LICENSED SOFTWARE OR SERVICES SHALL MEET CUSTOMER'S REQUIREMENTS.

8.6. Customer Warranty. Customer warrants that Customer (a) has the power and authority to enter into this Agreement and bind each Licensed User to the confidentiality and use restrictions set forth herein; and (b) shall use its best efforts to protect the security of the Licensed Software and Cloud Services.

9. **LIMITATION OF LIABILITY**. MEDIWARE'S MAXIMUM LIABILITY FOR DAMAGES TO CUSTOMER FOR ANY CAUSE WHATSOEVER ARISING UNDER OR RELATED TO THIS AGREEMENT, IS LIMITED TO THE FEES PAID UNDER THE ORDER FORM FOR THE AFFECTED SOFTWARE OR SERVICES DURING THE 12 MONTHS PRECEDING THE EVENT GIVING RISE TO A CLAIM. NEITHER MEDIWARE NOR ITS LICENSORS SHALL BE LIABLE FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE DAMAGES, OR LOST PROFITS, BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT LIABLITY, OR ANY OTHER LEGAL THEORY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY A THIRD PARTY AGAINST CUSTOMER. Mediware shall not be deemed to be engaged, directly or indirectly, in the practice of medicine or the dispensing of medical services, nor shall it be responsible or liable for the use, application or interpretation of any information, results or product generated by or resulting from the Licensed Software or Services or arising from the Customer's use of the Licensed Software or Services.

10. **INDEMNIFICATION**.

10.1. Mediware Indemnity. Mediware shall defend, indemnify and hold Customer and its officers, directors, and employees, harmless from and against any third party claims, suits, liabilities, obligations, judgments, and causes of action ("Third Party Claims") and associated costs and expenses (including reasonable attorneys' fees) to the extent arising out of any claim that the Licensed Software or Cloud Services infringes any currently existing United States patent or copyright, or misappropriates any trade secret, of any third party. If Customer's use of the Licensed Software or Cloud Services is finally enjoined, Mediware shall, at its sole

option and expense, and as Customer's sole and exclusive remedy, either: (a) secure for Customer the right to continue to use the Licensed Software or Cloud Services; (b) replace, modify or correct such Licensed Software or Cloud Services to avoid such infringement, or (c) terminate the Agreement and refund to Customer a pro rata portion of the Licensed Software license fees amortized over a five (5) year straight line depreciated basis and any prepaid amounts for Cloud Services not yet performed. Mediware's indemnification obligations shall not apply if the Third Party Claim results from: (i) modifications of the Licensed Software or Cloud Services by Customer or third parties; (ii) use of the Licensed Software or Cloud Services with non-Mediware software or equipment; (iii) use of the Licensed Software or Cloud Services in violation of this Agreement, Applicable Law, or in conformance with the Documentation; or (iv) use of anything other than the most current release of the Licensed Software, if the infringement could be avoided by use of the current release.

10.2. Customer Indemnity. Customer shall defend, indemnify and hold Mediware and its officers, directors, and employees harmless from and against any Third-Party Claim and associated costs and expenses (including reasonable attorneys' fees) to the extent arising out of or resulting from Customer's use of the Licensed Software, Test Scripts and Cloud Services, or any claim by any party receiving services from Customer in connection with the Licensed Software or Cloud Services.

10.3. Indemnification Procedures. To be indemnified, the party seeking indemnification must: (i) give the other party timely written notice of such Third-Party Claim (unless the other party already has notice); provided, however, that failure to give such notice will not waive any rights of the indemnified party except to the extent that the rights of the indemnifying party are prejudiced thereby; (ii) give the indemnifying party authority, information and assistance for the Third-Party Claim's defense and settlement. The indemnifying party has the right, at its option, to defend the Third-Party Claim at its own expense and with its own counsel. The indemnified party has the right, at its option, to join in the defense and settlement of such Third-Party Claim and to employ counsel at its own expense, but the indemnifying party shall retain control of the defense. The indemnifying party has the right to settle the claim so long as the settlement does not require the indemnified party to pay any money or admit any fault without the indemnified party's prior written consent, which will not be unreasonably withheld, conditioned or delayed.

11. TERM AND TERMINATION OF LICENSE AND AGREEMENT.

11.1. Term. If applicable, the term of the license to the Licensed Software and Cloud Services is set forth in an Order Form. This Agreement shall terminate when the license to all Licensed Sofware licensed under this Agreement terminates, all Services expire or are terminated, or sooner as provided in Section 11.

11.2. Termination. This Agreement remains in effect until all Licensed Software and Services expire or are terminated in accordance with this Agreement. Either Party may terminate this Agreement and the licenses granted herein if: (i) the other Party materially breaches this Agreement and fails to cure such breach within 60 days after receipt of written notice of the same, except in the case of failure to pay fees when due, which must be cured within 10 days after receipt of written notice from Mediware; or (ii) the other Party becomes the subject of a voluntary proceeding relating to insolvency, receivership, liquidation, bankruptcy or composition for the benefit of creditors and such petition or proceeding is not dismissed within 60 days of filing. Failure to use the Licensed Software and Updates thereto in accordance with Applicable Law is a material breach of this Agreement.

11.3. Effect of Termination. Upon termination of this Agreement, Customer shall immediately cease all use of the Licensed Software, Sublicensed Software and Cloud Services, the licenses granted and all other rights of Customer under this Agreement shall terminate and revert to Mediware. Customer shall, within 10 days following such termination, return or destroy to Mediware all magnetic media or tangible

items and material containing the Licensed Software and its Documentation, all Mediware Confidential Information and certify such return or destruction in writing to Mediware.

11.4. Survival. The following sections shall survive termination or expiration of this Agreement: Articles 9, 10, 11, 12 and 14; Sections 8.4 through 8.6**,** as well as any obligation to pay fees arising prior to termination or expiration. In addition, restrictions on use of the Licensed Software and related obligations regarding use in conformance with laws and applicable accreditation standards shall survive as long as the license survives.

12. **CONFIDENTIAL INFORMATION**. Each Party shall (i) secure and protect the Confidential Information using the same degree or greater level of care that it uses to protect such Party's own confidential information, but no less than a reasonable degree of care; (ii) use the Confidential Information of the other Party solely to perform its obligations or exercise its rights under this Agreement; (iii) require their respective employees, agents, attorneys, and independent contractors who have a need to access such Confidential Information to be bound by confidentiality obligations sufficient to protect the Confidential Information; and (iv) not transfer, display, convey or otherwise disclose or make available all or any part of such Confidential Information to any third party. Either party may disclose the other party's Confidential Information to the extent required by Applicable Law or regulation, including without limitation any applicable Freedom of Information or sunshine law, or by order of a court or other governmental entity, in which case the disclosing party shall notify the other party as soon as practical prior to such disclosure and an opportunity to respond or object to the disclosure.

13. **REGULATORY COMPLIANCE**.

13.1. General. Mediware shall make available to the Secretary of Health & Human Services or Comptroller General of the United States its books, documents, and records necessary to verify the nature and extent of the costs of those Services. Said access shall be limited to a period of four (4) years after the provision of the applicable services hereunder.

13.2. HIPAA. The parties agree to the terms of the Business Associate Exhibit that is attached hereto as Exhibit D.

14. **GENERAL PROVISIONS**.

14.1. Force Majeure. Neither Party shall be liable for any loss, damages or penalty (other than the obligation to pay money) resulting from any failure to perform due to causes beyond the reasonable control of such Party, including, but not limited to: supplier delay, acts of God, labor disputes, terrorism, war, unavailability of components, acts of governmental authorities or judicial action, or material interruption in telecommunications or utility service. The delayed party shall perform its obligations within a reasonable time after the cause for the failure has been remedied, and the other party shall accept the delayed performance.

14.2. Data Use. Notwithstanding any other terms to the contrary in a prior or contemporaneous agreement, Customer grants Mediware permission to use information about Customer's business and experience to help Mediware to provide the Licensed Software and/or Services to Customer and to enhance the Licensed Software and/or Services. Customer grants Mediware permission to combine Customer's business data, if any, with that of others in a way that does not identify Customer or any individual personally. Customer also grants Mediware permission to share or publish summary results relating to research data and to distribute or license such data to third parties.

14.3. Injunctive Relief. Customer acknowledges that any breach by Customer of Article 2 or 12 of this Agreement shall cause Mediware irreparable harm not compensable with money damages, and that in the event of such breach, Mediware shall be entitled to seek injunctive relief, without bond, from any court of competent jurisdiction.

14.4. Assignment. Neither Party shall assign its rights, duties or obligations under this Agreement without the prior written

consent of the other Party and such consent shall not be unreasonably withheld. Notwithstanding the foregoing, Mediware may assign this Agreement to an affiliate or in connection with any merger, reorganization or sale of substantially all of Mediware's assets or other change of control transaction without any consent from Customer.

14.5. Relationship of the Parties. Mediware is an independent contractor, and none of Mediware's employees or agents shall be deemed employees or agents of Customer. Nothing in this Agreement is intended or shall be construed to create or establish any agency, partnership or joint venture relationship between the Parties.

14.6. Export. Customer agrees to comply with all export and re-export restrictions and regulations of the Department of Commerce or other United States agency or authority, and not to transfer, or authorize the transfer of, the Licensed Software or the Sublicensed Software to a prohibited country or otherwise in violation of any such restrictions or regulations.

14.7. Notices. All notices, requests, demands or other communication required or permitted to be given by one Party to the other under this Agreement shall be sufficient if sent by certified mail, return receipt requested. The sender shall address all notices, requests, demands or other communication to the recipient's address as set forth on the first page of this Agreement, and in the case of Mediware, to the attention of Senior Vice President and General Counsel and in the case of Customer, to the attention of _____.

14.8. Severability. If any provision of this Agreement or any Order Form adopted in connection herewith is held invalid or otherwise unenforceable, the enforceability of the remaining provisions shall not be impaired thereby and the illegal provision shall be replaced with a legal provision that encapsulates the original intent of the Parties.

14.9. Entire Agreement; Amendment; Waiver. This Agreement constitutes the entire agreement between the Parties and supersedes any prior or contemporaneous agreement or understandings with respect to the subject matter of this Agreement. In the event of a conflict between this Agreement and an Order Form, the Agreement shall control. This Agreement shall be construed as if both Parties had equal say in its drafting, and thus shall not be construed against the drafter. This Agreement may be modified only by a written agreement signed by all of the Parties hereto. No waiver or consent granted for one matter or incident will be a waiver or consent for any different or subsequent matter or incident. Waivers and consents must be in writing and signed by an officer of the other Party to be effective.

14.10. Limitation on Actions. Neither party may bring any action arising out of or otherwise associated with this Agreement or the rights granted hereunder (other than failures to pay) more than two years after the cause of action accrues.

14.11. Discounts. Customer is reminded that if the purchase includes a discount or loan, Customer may be required to fully and accurately report such discount or loan on cost reports or other applicable claims for payment submitted under any federal health care program, including but not limited to Medicare and Medicaid, as required by federal law – see 42 CFR 1001.952 (h).

14.12. Purchase Orders; Acceptance of Quotes. If Customer submits its own terms in Customer's acceptance of a price quotation or in a purchase order, which add to, vary from, or conflict with the terms herein, any such terms are of no force and effect and are superseded by this Agreement.

14.13. Governing Law. This Agreement will be governed by, construed and interpreted in accordance with the laws of the State of Kansas, excluding its rules of conflicts of law. Both parties hereby consent and submit to the courts located solely in the state of Kansas.

14.14. Non-Solicitation. During the term of this Agreement and for a period of one (1) year thereafter, Customer agrees not to hire, directly or indirectly, any employee or former employee of Mediware, without obtaining Mediware's prior written consent.

14.15. Counterparts. This Agreement may be executed in any number of counterparts, each of which shall be an original, and such counterparts together shall constitute one and the same instrument. Execution may be effected by delivery of email or facsimile of signature pages, which shall be deemed originals in all respects.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the day and year first above written.

_____:	**MEDIWARE HUMAN & SOCIAL SERVICES, INC.:**
_____	_____
(SIGNATURE)	(SIGNATURE)
_____	_____
(PRINT NAME)	(PRINT NAME)
_____	
_____	_____
(TITLE)	(TITLE)
_____	_____
(DATE)	(DATE)

EXHIBIT A

14.16. **"Applicable Law"** means any law or regulation, or related administrative agency requirement affecting or governing the features, functionality, use, testing or Validation of any of the Licensed Software, including validation requirements affecting Regulated Licensed Software.

14.17. **"Cloud Services"** means, collectively, the Mediware software as a service offering listed in an Order Form and defined in the Documentation. The term "Cloud Services" does not include Professional Services.

14.18. **"Concurrent User"** means each Customer workstation able to simultaneously access the System at any given moment, for purposes of updating the System.

14.19. **"Confidential Information"** means (i) the source and object code of all components of the System, (ii) the Documentation, (iii) the Test Scripts, (iv) the design and architecture of the database, (v) the terms and conditions of this Agreement, and (vi) all other information of a confidential or proprietary nature disclosed by one Party to the other Party in connection with this Agreement which is either (x) disclosed in writing and clearly marked as confidential at the time of disclosure or (y) disclosed orally and clearly designated as confidential in a written communication to the receiving Party within 7 days following the disclosure. "Confidential Information" shall not include information (a) publically available through no breach of this Agreement, (b) independently developed or previously known to it, without restriction, prior to disclosure by the disclosing Party, (c) rightfully acquired from a third party not under an obligation of confidentiality.

14.20. **"Designated Platform"** means the required operating environment for the Licensed Software, including all necessary hardware and software components, specified in an applicable Order Form or Documentation.

14.21. "**Documentation"** means the most recent documentation of the functional operation of the Licensed Software and Cloud Services; provided that if the Licensed Software is a product that is cleared by the FDA, Documentation means the documentation provided to the FDA in connection with the FDA Clearance.

14.22. **"FDA Clearance"** means the 510(k) clearance received by Mediware from the Food and Drug Administration that authorizes the commercialization of the Regulated Licensed Software and sets forth the specific parameters of use for the Regulated Licensed Software on the Designated Platform.

14.23. **"First Productive Use"** means the day Customer begins using any part of the System or Cloud Services in a live production environment.

14.24. **"Hardware"** means any computer hardware (including, as applicable, embedded or bundled third-party software provided as a component of such hardware) identified in an Order Form to be purchased by Customer from Mediware.

14.25. "**Licensed User**" means a permitted user of Licensed Software, Sublicensed Software and Cloud Services as described in the applicable Order Form.

14.26. **"Licensed Software"** means the object code version of computer programs developed by Mediware listed in Section I of an Order Form, including Updates furnished to Customer by Mediware pursuant to this Agreement or any Order Form, but excluding all Sublicensed Software or third-party software.

14.27. **"Order Form"** means a work authorization executed by the Parties from time to time, including the Order Forms(s) attached hereto setting forth the items being purchased by the Customer, scope of use, pricing, payment terms and any other relevant terms, which will be a part of and be governed by the terms and conditions of this Agreement.

14.28. **"Professional Services"** means, collectively, the implementation, installation, data conversion, validation, or training services provided by Mediware under or in connection with this Agreement.

14.29. **"Program Error"** means an error or bug preventing the Licensed Software from operating in accordance with the Documentation in all material respects.

14.30. **"Services"** means the Cloud Services, Professional Services and the Support Services set forth in an Order Form.

14.31. **"Site"** means each of the Customer facility or facilities specified in an Order Form and for whom Customer (a) owns at least 50%, or (b) has the right to determine management direction.

14.32. **"Support Services"** shall mean the services to keep the Licensed Software in working order and to sustain useful life of the Licensed Software, including Updates and specified in an Order Form.

14.33. **"Sublicensed Software"** shall mean those programs provided to Mediware by a third party, which Mediware sublicenses to Customer hereunder, for use with the Licensed Software, as specified on an Order Form, and subject to the limitations set forth in this Agreement and any other applicable third party terms and conditions.

14.34. **"System"** shall mean the Licensed Software (all or less than all of the Licensed Software) and Sublicensed Software, if any, and any Updates thereto.

14.35. **"Test Scripts"** means Mediware's test scripts designed by Mediware to assist in Customer's Validation of certain Regulated Licensed Software.

14.36. **"Update"** means any error corrections, bug fixes, enhancements, and/or new features to the Licensed Software or Test Scripts that Mediware makes generally commercially available to its customers who have a current Maintenance and Support Agreement. Updates do not include modules, scripts or software that Mediware prices or markets separately.

14.37. **"Validation"** means the procedure performed by Customer to validate the Licensed Software pursuant to certain rules and regulations promulgated by the Food and Drug Administration.

14.38. "**Warranty Period**" means twelve months from the execution of the applicable Order Form, unless a different period is set forth in an Order Form.

14.39. **"Work Product"** means any technology, documentation, software, procedures developed, conceived or introduced by Mediware in the course of Mediware performing Services, whether acting alone or in conjunction with Customer or its employees, Licensed Users, affiliates or others, designs, inventions, methodologies, techniques, discoveries, know-how, show-how and works of authorship, and all United States and foreign patents issued or issuable thereon, all copyrights and other rights in works of authorship, collections and arrangements of data, mask work rights, trade secrets on a world-wide basis, trademarks, trade names, and other forms of corporate or product identification, and any division, continuation, modification, enhancement, derivative work or license of any of the foregoing.

EXHIBIT B
LICENSED SOFTWARE SUPPORT TERMS

1. Mediware Customer Support Service Level Agreement Guidelines (SLA)

The Mediware Support SLA guidelines are based on support case priority levels which are driven by business impact to the Mediware user community, and provide guidance to the Customer Support team with regard to response timeframes.

14.40. Support Case Priority Tracking and Response Guidelines

The priority level of a support case is determined, based on the business impact to the user community, or affected users and groups. After setting the support case priority, automated triggers and reporting from the Mediware case tracking system become available to Mediware Support Team and management on each case entered into the Mediware Customer Relationship Management system. The case priority tracking levels, their definition, and guidelines for response can be found in the table below.

Priority Level	Priority Level Description	Initial Response Timeframe
Password Reset	Request for Password Reset	Within 1 Hour during operating hours
Medium	Low business impact, minor operational issue or question, product or operational questions, product issue which a reasonable workaround exist, training questions, or enhancement suggestion; resolution not required for continuity of customer's operation	Within 1 Day during operating hours
High	One or more features do not seem to be working as designed; workarounds may be available, timely resolution will prevent manual process or lost business value.	Within 4 hours during operating hours
Urgent	Urgent business impact, solution is not functioning at an acceptable level for the majority of users; customer's operation is being seriously impacted, OR may refer to a request where resolution is key to a business critical time-sensitive task. Session Disconnects may be included in this category.	Within 2 hours during operating hours
Critical	Mission Critical Business Impact, solution is completely unavailable or unresponsive; the customer's operation is severely impacted.	Within 1 hour during operating hours

* If multiple customers are impacted, mass communication will be sent in lieu of individual responses.
** The above are "guidelines" only for case SLA performance, and response may vary on a case-by-case basis. Guidelines are subject to change over time.

2. Protocol for Accessing Mediware Support

Mediware's support team provides telephone, email, and Internet-based support. All customer inquiries are logged as cases in Mediware's Support Center CRM system and assigned unique identification numbers for tracking.

The Mediware Customer Support Team includes Customer Care Analysts (CCAs).

The Mediware Customer Support Team will provide support help in many areas, such as answering user questions, logging system enhancement requests, handling patch and update notifications, and providing assistance in troubleshooting problems.

14.41. Mediware Customer Support Hours of Operation

Mediware Customer Support is open Monday – Friday, 8 AM – 5 PM ET (excluding Company Holidays).

14.42. Contact and Case Creation Methods

The Mediware Customer Support Team business processes and data recording utilize the support case record. All assistance provided is recorded in the case as it is tracked through the various stages to completion. Mediware advises customers to always create a support case whenever a response is needed from Mediware Customer Support.

Mediware offers three methodologies to create support cases:

1. Mediware Customer Support Community - https://portals.force.com/mediware/
2. Email – customersupport@mediware.com
3. Phone Support - 1-800-318-7260

14.42.1 Mediware Customer Support Community

The Mediware Customer Support Community is an automated solution for system administrators to manage support tickets. The community provides system administrators an online tool to create and manage cases with the Mediware Customer Support team. Mediware Customer Support uses customer information provided through the community to understand and effectively respond to customer needs, streamline and simplify support efforts, improve customer satisfaction, and improve abilities to manage Mediware support requests in a timely and effective manner. Through the portal, system administrators have around-the-clock access to real-time status of their submitted support cases.

14.42.2 Email: customersupport@mediware.com

Sending an email to the Mediware Customer Support Team email address will automatically generate a support case in the CRM system. Users may email Mediware at any time at customersupport@mediware.com and the Mediware Customer Support Team will communicate with the customer, including through use of the case reporter, through the case record. Users will receive a response in their inbox and may reply via the email thread throughout the support case life cycle. All email activity is stored within the case record.

14.42.3 Phone: 1-800-318-7260 (toll-free)

Mediware provides toll-free telephone-based support to customers, recognizing that not all incidents are easily communicated by online case entry alone. Phone support is suggested for situations where customers have difficulty articulating a need via the Customer Community or if they need to speak directly to a support representative during business hours. Mediware Customer Care Analysts answer incoming calls as designated in a queue to facilitate user responsiveness.

14.43. Remote Session Sharing Tools

Mediware also provides a collaborative, web-based access tool to allow sharing of desktops between support representatives and end users during phone conversations. This ability to demonstrate and view enables Mediware to provide an interactive support experience that further contributes to an interactive customer experience. In addition to walking through illustrative examples and results of their analyses, the support team can use the tool to shadow customer user sessions to further understand the question or problem under consideration. This tool enables the support team to:

- Accelerate diagnosis and problem solving.

- Troubleshoot issue on customer hardware and solutions when needed.
- Provide real-time analysis while a problem is occurring.
- Demonstrate product features when appropriate.

14.44. After Hours Case Submission Support

The Mediware Customer Support Community, email support, and phone-based case reporting (to voice message) are all available methods to log cases after hours. 24 x 7, Customers can use the Customer Support Community to report/view support cases, and may report cases via the community, email, and phone methodologies. Mediware Customer Support will follow-up on cases submitted after-hours during normal business hours.

Mediware also has 24/7 monitoring of the entire hosting infrastructure and responds to critical alerts after hours.

EXHIBIT C
ADMINISTRATIVE ACCESS ADDENDUM

1. Grant of Limited Administrative Access; Protection of Privileges. Subject to the terms and conditions herein and in the Agreement, Mediware agrees to provide Customer with limited, remote administrative access for up to four (4) Administrators (defined below) to limited aspects of Mediware's portal environment, solely to the extent necessary for Customer to manage accounts of the authorized individual users of the Software (the "Authorized Purpose"). The degree of access shall be determined by Mediware, in its sole discretion, but at a minimum, the Authorized Purpose shall include; (i) providing Customer's Administrators with the ability to remotely access, via the web, Mediware's portal administration, (ii) creating and managing Customer's user accounts, (iii) setting user access and security configuration, (iv) create and edit portal user accounts, (v) inactivate portal user accounts, (vi) reset portal user passwords, (vii) manage user access to applications, and (viii) add website links to portal view and post announcements on the portal. Customer and the Administrators administrative access shall be for the Authorized Purpose, and for no other purpose, and Customer (including the Administrators) are expressly prohibited from using such access to, among other things, change the number of authorized licensed users, change, in any way, the license grant authorized in the Agreement, or access any portion of the Software and/or the Software environment not expressly necessary to accomplish the Authorized Purpose. Customer and the Administrators shall appropriately safeguard the administrative access rights granted hereunder to prevent unauthorized use. Customer shall only provide administrative access to employees who are, prior to being given such access, identified to Mediware in writing, and approved by Mediware (such identified and approved employees, the "Administrators"). Customer shall notify Mediware in writing of any proposed change in the Administrators prior to granting/changing such access, and Customer shall ensure that Administrators who leave Customer's employ, or who are otherwise removed from the role of an Administrator are denied access immediately upon such change. Customer (including the Administrators) shall not abuse or misuse the administrative access granted hereunder, and any abuse shall constitute a breach of this Addendum.

2. Liability for Administrative Access.

    a. *Customer Liability.* Notwithstanding anything to the contrary, Customer shall, without limitation, defend, indemnify and hold Mediware harmless from any and all claims, expenses liabilities, penalties and costs (including, without limitation, reasonable attorney's fees and court costs) arising out of or related to the administrative access granted under this Exhibit.

    b. *No Liability for Mediware*. NOTWITHSTANDING ANYTHING TO THE CONTRARY, IN NO EVENT SHALL MEDIWARE (1) HAVE ANY LIABILITY WHATSOEVER IN CONNECTION WITH THIS EXHIBIT, OR THE ACCESS GRANTED HEREUNDER, OR (2) BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, IN CONNECTION WITH THIS ADDENDUM. SHOULD THE FOREGOING LIMITATION FAIL OF ITS ESSENTIAL PURPOSE, THEN MEDIWARE'S MAXIMUM, CUMMULATIVE LIABILTY ARISING UNDER OR IN CONNECTION WITH THIS ADDENDUM SHALL NOT EXCEED ONE THOUSAND DOLLARS ($1,000.00).

3. Termination. The rights granted in this Exhibit may be terminated early, without cause and for any reason, by Mediware upon five (5) days' prior written notice to Customer. In addition, and notwithstanding anything to the contrary, Mediware may immediately terminate and/or suspend the rights granted under this Exhibit for cause; (A) upon Customer's or an Administrator's breach of this Exhibit, or (B) in the event Mediware has reason to believe, in its sole discretion, that the security or integrity of

Mediware's software, services or networks are at risk. In the event Customer's administrative access is terminated, Mediware agrees to perform such services that were previously performed by Customer under this Exhibit. Mediware reserves the right to charge a fee for such services. Such fee shall be mutually agreed upon by Customer and Mediware. Any termination or suspension permitted hereunder shall be without penalty to Mediware. Termination of the rights under this Exhibit shall not operate to terminate the Agreement, unless this Addendum is terminated by Mediware for cause.

EXHIBIT D

BUSINESS ASSOCIATE AGREEMENT

BACKGROUND

A. Covered Entity and Mediware have entered into a certain License Agreement dated _____ (such agreement is the "Agreement"), pursuant to which Covered Entity has licensed software from Business Associate and Business Associate provides implementation, maintenance, support and other services to Covered Entity.

B. Covered Entity possesses Protected Health Information that is protected under the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191) and the regulations promulgated thereunder by the United States Department of Health and Human Services (collectively, "HIPAA"), and is permitted to use or disclose such Protected Health Information only in accordance with HIPAA and the Regulations.

C. Business Associate may have access to and may receive Protected Health Information from Covered Entity in connection with its performance of services to under the Agreement.

TERMS

1. Definitions. All capitalized terms used but not otherwise defined in this Business Associate Agreement ("BAA") shall have the same meaning as those terms in the Regulations.

a. Business Associate shall mean Mediware Information Systems, Inc.
b. Covered Entity shall mean Customer.
c. Individual shall have the same meaning as the term "individual" in 45 CFR § 160.103 of the Regulations and shall include a person who qualifies as a personal representative in accordance with 45 CFR§ 164.502(g) of the Regulations.
d. Regulations shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E, Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 160 and Part 164, Subparts A and C; 45 CFR § 164.314, and the Health Information Technology for Economic and Clinical Health Act (HITECH), as it directly applies, as in effect on the date of this BAA.
e. Protected Health Information shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
f. Required by Law shall have the same meaning as the term "required by law" in 45 CFR § 164.103 of the Regulations.
g. Secretary shall mean the Secretary of the Department of Health and Human Services or his/her designee.

2. Obligations and Activities of Business Associate.

a. Business Associate agrees to comply with the requirements of the Privacy and Security Rules directly applicable to Business Associates through the HITECH Act.
b. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this BAA, the Privacy and Security Rules, the Agreement, or as required by law. Such disclosures shall be consistent with the "minimum necessary" requirements of the Regulations.
c. Business Associate agrees to use appropriate safeguards to protect against the use or disclosure of the Protected Health Information other than as provided for by this BAA or the Agreement.
d. Business Associate agrees to mitigate, to the extent reasonably practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this BAA.

e. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by the BAA of which it becomes aware.
f. Business Associate shall notify Covered Entity of a breach of the Privacy Rule relating to the impermissible use or disclosure of Protected Health Information provided to the Business Associate for purposes of carrying out its obligations under the Agreement. Unless otherwise required by law or agreed to by the parties, it shall be the responsibility of Covered Entity to communicate with affected individual(s), the Secretary and the media information regarding the unintended use or disclosure.
g. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity agrees to the same or similar restrictions and conditions that apply through this BAA to Business Associate with respect to such information.
h. If Business Associate maintains Protected Health Information in a Designated Record Set for Covered Entity, Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner reasonably designated by Covered Entity, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524 of the Regulations. In the event a request for access is delivered directly to Business Associate by an Individual, Business Associate shall as soon as possible, forward the request to Covered Entity.
i. If Business Associate maintains Protected Health Information in a Designated Record Set for Covered Entity, Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 of the Regulations at the request of Covered Entity or an Individual, and in the time and manner reasonably designated by Covered Entity. In the event a request for amendment is delivered directly to Business Associate by an Individual, Business Associate shall as soon as possible, forward the request to Covered Entity.
j. Business Associate agrees to make internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary, in a time and manner reasonably designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Regulations.
k. Business Associate agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528 of the Regulations.
l. Business Associate agrees to provide to Covered Entity or an Individual, in time and manner reasonably designated by Covered Entity, information collected in accordance with Section 2(k) of this BAA, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528 of the Regulations. In the event a request for accounting is delivered directly to Business Associate by an Individual, Business Associate shall as soon as possible, forward the request to Covered Entity.

3. Permitted Uses and Disclosures by Business Associate

a. Except as otherwise limited in this BAA, Business Associate may use or disclose Protected Health Information to perform functions, activities or services for, or on behalf of, Covered Entity in connection with the BAA and any other agreements in effect between Covered Entity and Business Associate, including without limitation the provision of software implementation and support services, provided that such use or disclosure would not violate the Regulations if done by Covered Entity.

b. Except as otherwise expressly limited in this BAA, Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

c. Except as otherwise expressly limited in this BAA, Business Associate may disclose Protected Health Information for disclosures that are Required By Law, or if Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person

notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

d. Except as otherwise expressly limited in this BAA, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR § 164.504(e)(2)(i)(B).

e. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR § 164.502(j)(1).

4. Termination.

a. Except as otherwise provided herein, this BAA shall terminate upon termination of the Agreement.
b. Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate of this BAA, Covered Entity may:
    1. Provide a reasonable opportunity for Business Associate to cure the material breach or end the material violation and if Business Associate does not cure the material breach or end the material violation within a reasonable time, Covered Entity may terminate this BAA and the provisions of the Agreement that require or permit Business Associate to access Protected Health Information;
    2. If Business Associate has breached a material term of this BAA and cure is not possible, immediately terminate this BAA and the provisions of the Agreement that require or permit Business Associate to access Protected Health Information; or
    3. If neither termination nor cure is feasible, report the violation to the Secretary.

    If Covered Entity breaches, Business Associate may terminate this BAA and any Underlying Agreement 30 days after written notice.

c. Effect of Termination.
    1. Except as provided in paragraph (2) of this section, upon termination of this BAA, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.
    2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. In such event, Business Associate shall extend the protections of this BAA to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. Except as provided herein, any termination of the maintenance program or provisions of the Agreement that permit Business Associate to access Protected Health Information shall not affect the parties other obligations or rights under the Agreement.

5. Obligations of Covered Entity.

a. Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.
b. Covered Entity shall notify Business Associate of any changes in or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect the Business Associate's use or disclosure of protected health information.
c. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

d. Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR part 164 if done by Covered Entity.

6. Electronic Data Security. Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any electronic Protected Health Information that it creates, receives, maintains or transmits to or on behalf of Covered Entity as required by the Regulations. Business Associate further agrees to ensure that any agent, including a subcontractor, to whom it provides such information, agrees to implement reasonable and appropriate safeguards to protect it. Business Associate agrees to promptly report to Covered Entity any security incident of which it becomes aware.

7. Miscellaneous.

a. De-Identified Information. Business Associate may de-identify Protected Health Information obtained by Business Associated under this BAA in compliance with 45 CFR § 164.502(d) and 45 CFR § 164.514(a) and (b). Pursuant to 45 CFR § 164.502(d)(2), de-identified information does not constitute Protected Health Information and is not subject to the terms of this BAA.
b. Data Use. Business Associate may use and disclose Protected Health Information obtained by Business Associate under this BAA to create a limited data set without any of the identifiers listed in 45 CFR § 164.514(e) ("Limited Data Set") for research, public health, and health care operations purposes. Business Associate may not use or further disclose a Limited Data Set for any other purpose, except as may otherwise be Required by Law. Business Associate must use appropriate safeguards to prevent use or disclosure of a Limited Data Set other than as provided for herein. Business Associate must report to Covered Entity any use or disclosure of a Limited Data Set not provided for herein of which Business Associate becomes aware. Business Associate must ensure that any agents to whom Business Associate provides a Limited Data Set agree to the same or substantially similar restrictions and conditions that apply to Business Associate with respect to such information. Business Associate may disclose a Limited Data Set to any recipient that agrees to the same or substantially similar restrictions and conditions that apply to Business Associate with respect to such information. With respect to any particular Limited Data Set, Business Associate will not use the Limited Data Set in such a way as to identify any individual whose data is incorporated in the Limited Data Set or to contact any such individual.
c. Changes to Regulations. If the Regulations are amended in a manner that would alter the obligations of Mediware as set forth in this BAA, then the parties agree in good faith to negotiate mutually acceptable changes to the terms set forth in this BAA.
d. Survival. The respective rights and obligations of Business Associate under Section 4(c) of this BAA shall survive the termination of this BAA.
e. Minimum Necessary. Covered Entity shall only provide a minimum amount of Protected Health Information necessary for the Business Associate to satisfy its obligations under the Agreement.
f. Interpretation. Any ambiguity in this BAA shall be resolved to permit compliance with the Regulations.
g. Incorporation. Except for Covered Entity, no third party may rely on the terms, conditions, rights, remedies or obligations hereunder. The terms of this BAA are fully incorporated in and subject to the terms of the Agreement.

HOSTING SERVICE LEVELS

This Exhibit B-1 sets forth certain Mediware hosting service requirements. From time-to-time, these obligations may change upon notice by Mediware to Customer. Such changes are not intended to materially change SaaS Provider's obligations or Client's rights, but may be necessitated by changing technologies, industry practices, or other circumstances.

CLOUD SERVICES – HOSTING

1. Definitions
The following terms have the following meaning. Capitalized terms not defined herein, shall have the meaning given in the Agreement.

1.1 "**Non-Core System Functionality**" means functionality that does ***not*** require real time availability for effective use of the Cloud Services. This explicitly includes, but is not limited to, reporting and background batch processing. Non-Core System Functionality availability is explicitly excluded from the calculation of Availability.

1.2 "**Core System Functionality**" means functionality that does require real time availability for effective use of Cloud Services. Core system functionality includes all features required to commence a user session and performs end user operations, including create, read, update and delete operations.

1.3 "**Scheduled Downtime**" means the total amount of time during any calendar year, measured in minutes, during which the Core System Functionality is unavailable for access Customer's active Licensed Users according to the Access Protocols, due to scheduled system maintenance performed by or on behalf of Mediware.

1.4 "**Unscheduled Downtime**" means the total amount of time during any calendar year, measured in minutes, during which the Core System Functionality is unavailable for access by Customer's Licensed Users according to the Access Protocols, other than for Scheduled Downtime and the exceptions otherwise stated in the Agreement. Unscheduled Downtime will not include, without limitation, any downtime arising from: (i) Customer's breach of any provision of the Agreement; (ii) non-compliance by Customer with any provision of the Agreement; (iii) incompatibility of Customer's equipment or software with the Cloud Services; (iv) poor or inadequate performance of Customer's systems; (v) Customer's equipment failures; (vi) acts or omissions of Customer or its Licensed Users, contractors or suppliers; (vii) telecommunication or transportation difficulties; (viii) Customer's network and internet service provider, (ix) public internet, (x) security exposure, or (xi) force majeure (as described in the Agreement). In the event of a "Disaster" or Customer's non-compliance with the Agreement, the Availability Service Standard (and related fee reductions) shall not apply.

1.5 "**Disaster**" means a catastrophic event (or series of events that are collectively catastrophic) not caused by Mediware that results in significant or potentially significant downtime or disruption of the production environment and requires Mediware to invoke its Disaster Recovery plan. Mediware has the sole and exclusive right to declare a disaster.

1.6 "**Availability**" means the percentage determined as follows:

$$\textbf{Availability} = \frac{\textbf{(Total Annual Time - Unscheduled Downtime)}}{\textbf{Total Annual Time}} \times \textbf{100}$$

NOTE: "**Total Annual Time**" is deemed to include all minutes in the relevant calendar year excluding scheduled downtime as described above.

1.7 **"Access Protocols"** means industry standard internet access protocols through which Mediware makes the Cloud Services accessible to the Customer which includes, unless otherwise specified by the product or service contract for, HTTPS and FTPS.

1.8 **"Disaster Recovery"** means Mediware's process to restore Availability in the event that Mediware declares a Disaster.

1.9 **"Live/Production Instance"** means Customer and/or product URLs and the associated technology environment that is provided as part of the Cloud Services for accessing live data after the First Productive Use date and does not include any other instances that may be used for testing, training, development, staging or any purpose.

2. AVAILABILITY SERVICE STANDARD

Following First Productive Use of the Cloud Services, the Availability period will begin and is applicable to Live/Production Instances only. This period will begin with the First Productive Use by Customer and continue throughout the applicable subscription term. During the Term, Mediware will provide Customer with the following, after First Productive Use and during the term of this Agreement, Mediware will provide the Cloud Services via the Internet 24 hours a day, 7 days a week, in accordance with the terms of the Agreement.

Mediware will use commercially reasonable efforts to ensure that the Availability of the Cloud Services is at least **ninety-eight percent (98%)** during each full calendar year (the "***Availability Service Goal***"), provided that any Unscheduled Downtime occurring as a result of circumstances beyond Mediware's reasonable control shall not be considered Unscheduled Downtime. Unscheduled Downtime will not include, without limitation, any downtime arising from: (i) Customer's breach of any provision of the Agreement; (ii) non-compliance by Customer with any provision of the Agreement; (iii) incompatibility of Customer's equipment or software with the Cloud Services or Platform; (iv) poor or inadequate performance of Customer's systems; (v) Customer's equipment failures; (vi) acts or omissions of Customer or its Named Users, contractors or suppliers; (vii) telecommunication or transportation difficulties; (viii) Customer's network and internet service provider, (ix) public internet, (x) security exposure, or (xi) force majeure (as described in the Agreement). In the event of a "Disaster" or Customer's non-compliance with the Agreement, the Availability Service Goal does not apply.

3. SCHEDULED DOWN TIME

Periodically, Mediware will require Scheduled Downtime. Scheduled Downtime will normally be scheduled outside of normal business hours, with 72 hours' notice, or in the event of a more urgent need Mediware may give 12 hours' notice or less to resolve an immediate security need. Depending upon the immediacy of the Scheduled Downtime required, the down time may be rescheduled at the request of a Customer if reasonably possible. It is anticipated that there will be weekly Scheduled Downtime for system maintenance on Thursday mornings from 1:00AM to 3:00AM Eastern.

4. REPORTING UNSCHEDULED DOWNTIME

Customer is required to report any Unscheduled Downtime by calling Mediware Customer Support with the provided support number within one day of its occurrence. Mediware will exercise commercially reasonable efforts to respond to reports of Unscheduled Downtime by telephone or email acknowledgement within one hundred and eighty (180) minutes of each such report. The report will be assigned a case number for tracking purposes.

5. INTERNET CONNECTION DEPENDENCE

The performance and availability of the Cloud Services are directly dependent upon the quality of Customer's Internet connection. Mediware will aid the Customer in determining the quality of their Internet connection via the use of tools designed to measure throughput. This information may then be used to make an informed decision by Customer regarding Internet Service Provider ("ISP") selection. Failure of the Customer's Internet connection to maintain satisfactory throughput and latency is outside the scope of Mediware's responsibility, and should be addressed by Customer directly with the ISP. Mediware cannot be held responsible for Internet infrastructure failures, and as such this Exhibit B-1 only applies to those components within the Mediware's hosting services.

6. MEASUREMENT AND REPORTS

6.1 Monitoring and Measurement: Mediware will monitor Availability on an ongoing basis during the Term. This monitoring will be performed through a combination of monitoring tools. These tools are intended to serve as initial alert to Mediware. Mediware will conduct a series of tests to confirm Availability if it is alerted to potential Unscheduled Downtime.

- If an alerting mechanism reports that the Core System Functionality is unavailable, and the Customer confirms the unavailability as provided herein, then Unscheduled Downtime will be calculated as the time between when the initial notification or alert was confirmed until Mediware confirms availability has been restored.

- If an alerting mechanism reports that the Core System Functionality is potentially unavailable, but Mediware's tests and assessments confirms that is available, then the alert of potential unavailability will be dismissed and excluded from the calculation of Unscheduled Downtime.

6.2 System Performance Reports: Customer agrees that Mediware's monitoring and measurement method and standard Availability reports are the sole and exclusive methods of measuring Availability under this Exhibit. No other measure shall be accepted unless validated, and mutually agreed to in writing by both Parties before implementation.

7. CUSTOMER REQUIREMENTS

7.1 Minimum System: The service standards set forth in this Exhibit assume that Customer and its Licensed Users, meet and remain current with all minimum requirements relating to the Cloud Services. These minimum system requirements may vary over time due to Cloud Services version levels and other factors. As these requirements change, Mediware will inform the Customer such that the Customer can remain compliant with these requirements.

7.2 Additional Customer Obligations: Except as otherwise agreed between the Parties in a separate written agreement, Customer is responsible for (i) maintenance and management of its computer network(s), servers, software, and any equipment or services related to its receipt and use of the Cloud Services; and (ii) correctly configuring Customer's systems in accordance with the Access Protocols and minimum system requirements.

CLOUD SERVICES – SUPPORT

Mediware shall provide Customer and its Licensed Users with Email support and web-based and telephone support during the Subscription Term.

Standard Hours of Operation

Mediware customer service provides Customer with support available between the hours of 8:30 a.m. to 9:00 p.m. Eastern Standard Time Monday through Friday, excluding holidays. SaaS Provider reserves the right to be closed on other days from time-to-time throughout the year with notice prior to the actual day.
It is highly recommended that a focal point be established within the Customer's organization for reporting defects prior to submission to Mediware. This approach improves communication efficiency and reduces the potential for confusion.

Email Support

The Mediware Customer Service Center is staffed by qualified customer service representatives and can be reached through the following Email address:

support@mediware.com

Mediware will respond to all email requests within 24 to 48 hours (excluding weekends and holidays). This initial response may not contain a resolution to the issue depending on the severity and nature of the reported problem.

Email support is limited to questions directly related to the use of SaaS Provider Services, and does not include general

computer questions, or support for third-party software packages. Email support does not include Mediware Service demonstrations, personal tutorials or walkthroughs on functionality or features. It is assumed that the person contacting Mediware customer service has been fully trained and has read all applicable Documentation.

Telephone Support

The Mediware Customer Service Center can be reached at the following phone number:

800-318-7260

Customer service representatives will assist with the troubleshooting of issues that cannot be resolved by customer. If a customer service representative cannot be reached, then all voice mails will be responded to within 24 to 48 hours (excluding weekends and holidays).

Telephone support is limited to questions directly related to the use of Mediware Services, and does not include general computer questions, or support for third-party software packages. Telephone support does not include Mediware demonstrations or personal tutorials or walkthroughs on function or features. It is assumed that the person contacting Mediware customer service has been fully trained and has read all applicable Documentation.