



Provider Enrollment, Screening & Monitoring (PRESM) Business Continuity and Disaster Recovery Plan

Version: 1.1

Prepared for [REDACTED]

Submitted: September 28, 2020



TABLE OF CONTENTS

1	Introduction	9
1.1	Document Purpose.....	9
1.2	Document Scope	9
1.3	Document Audience	9
1.4	Constraints and assumptions	10
2	Business Continuity	10
2.1	Core business processes	10
2.2	Contingency Plan Triggers.....	15
2.3	Business Continuity Procedures	15
2.4	Business Functions Recovery Plan.....	16
2.5	Communication protocols and process for restoring operations	16
3	Disaster Recovery	16
3.1	Concept of Operations.....	16
3.1.1	System Description	16
3.1.2	Backup Plan, procedures, and schedules.....	20
3.1.3	Overview of Three Phases.....	22
3.1.4	Roles and Responsibilities.....	23
3.2	Activation and Notification	25
3.2.1	Activation Criteria and Procedure.....	25
3.2.2	Notification	25
3.2.3	Notification – External	26
3.3	Outage Assessment	26
3.4	Recovery.....	26
3.4.1	Sequence of Recovery Activities	26
3.4.2	Recovery Procedures	26
3.4.3	Recovery Escalation Notices/Awareness	28
3.5	Reconstitution	28
3.5.1	Validation Data Testing.....	28
3.5.2	Validation Functionality Testing.....	28
3.5.3	Recovery Declaration	28



3.5.4	Notification (users).....	28
3.5.5	Cleanup	29
3.5.6	Data Backup	29
3.5.7	Event Documentation	29
3.5.8	Deactivation	29
Appendix A. Definition of Terms and Acronyms		30
Appendix B. Referenced Documents		32
Appendix C. Personnel Contact List.....		33
Appendix D. Vendor Contact List		34
Appendix E. Detailed recovery procedures.....		36
Appendix F. System Validation Test Plan.....		37



TABLE OF FIGURES

Figure 1. System hardware/software architecture diagram.....	18
Figure 2. Business as Usual State of PRESM	19
Figure 3. Disaster Recovery State of PRESM	20
Figure 4. PRESM backup architecture.....	21
Figure 5. CloudEndure disaster recovery solution	22
Figure 6. PRESM Disaster Recovery Team structure.....	23



TABLE OF TABLES

Table 1: Core business processes risk and impact analysis.	10
Table 2: Assigned BCDRP Function / Assignees	23
Table 3: Recovery Procedure	26



REVISION HISTORY

Date	Version #	Assigned By	Version
07/20/2020	1.0	Leonid Marushevskyi/HHS Tech Group	Initial Submission



Sow Section# or Req ID#	Full Text Requirement or Description of SOW Section	Location of Where Requirement Addressed within Deliverable (Section, Page#, Paragraph/Item#)
Req ID# 119	The Contractor shall be able to demonstrate the ability to support requirements for backup and archiving consistent with Agency SLAs and CMS, State, and industry standards. The Contractor shall also adhere to data retention requirements cited in 45 CFR 164.316 and the State's Administrative Rules.	Section 3.1.2, page 19
Req ID# 149	The Contractor shall be responsible for backup and retention of data to include: 1. Daily incremental backups with retention of sixty-one (61) days. 2. Weekly incremental backups with retention of twelve (12) weeks. 3. Monthly full backups with retention of eighteen (18) months. 4. Annual full backups with retention of seven (7) years.	Section 3.1.2, page 19
Req ID# 163	The Contractor shall develop and maintain annually, a Business Continuity and Disaster Recovery Plan that must be in place before any Agency data is transferred or entered into the Solution. The Plan must contain procedures for data backup, restoration, and emergency mode operations in the event of: a. Hardware or Software Failures; b. Human Error; c. Natural Disaster; and/or d. Other unforeseeable emergencies. The Business Continuity and Disaster Recovery Plan must be approved by the Agency.	
Req ID# 164	The Contractor's Business Continuity portion of the Plan must include the following: a. Identification of the core business processes involved in the production solution. For each core business process include: 1) Identification of potential failures for the process; 2) Risk analysis; 3) Impact analysis; and 4) Definition of minimum acceptable levels of service/output. b. Definition of triggers for activating contingency plans. c. Procedures for activating any special teams for business continuity. d. A plan for recovery of business functions, units, processes, human resources, and technology infrastructure. e. Communication protocols and process for restoring operations in a timely manner.	Section 2, page 10
Req ID# 165	The Contractor's Disaster Recovery portion of the Plan must address, at a minimum: a. Retention and storage of backup files and software; b. Hardware backup for critical solution components; c. Facility backup; d. Backup for any telecommunications links and networks; e. Backup procedures and support to accommodate the loss of any online communications; f. A detailed file backup plan, procedures, and schedules, including rotation to an off-site storage facility. g. The	Section 3, page 15

	off-site storage facility must provide security of the data stored there, including protections against unauthorized access or disclosure of the information, fire, sabotage, and environmental considerations. h. An enumeration of the prioritized order of restoration for Contractor's proposed Solution. i. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
Req ID# 245	The Contractor shall develop operational procedures in coordination with other enterprise module vendors to restore system availability.	Section 3.2.2 Notification, page 25
Req ID# 300	The Contractor shall support the disaster recovery activities that will provide timely failover and create relevant documented policies and procedures to implement a recovery.	Section 3, page 15
Req ID# 301	The Contractor shall conduct an annual test of the Disaster Recovery and Business Continuity Plan and submit the Disaster Recovery/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the Agency.	Section 1.1, page 9
Req ID# 470	The Contractor shall provide the primary and disaster recovery facility(s) which will ensure security, performance and disaster recovery requirements outlined in the module scope of work.	Section 3.1.1, page 16
SLA ID# 14	Contractor must, in the event of an unscheduled Module Downtime, restore availability, using procedures approved in the Business Continuity and Disaster Recovery Plan within four (4) hours from the start of the unscheduled downtime.	Section 3.4, page 26
SLA ID# 36	Contractor shall provide an alternate business site if Contractor's primary business site becomes unsafe or inoperable. The alternate business site must be fully operational within two (2) business days of the primary business site becoming unsafe or inoperable.	Section 2.3, page 15

1 Introduction (Tracked changes turned on for my review- Barb)

1.1 Document Purpose

Information systems are vital to the [REDACTED] mission/business processes; therefore, services provided by WINGS PRESM must be able to operate effectively without interruption. This Business Continuity and Disaster Recovery Plan (BCDRP) establishes comprehensive procedures to recover WINGS PRESM quickly and effectively following a service disruption.

This BCDRP - establishes procedures to recover PRESM following a disruption. The following recovery plan objectives have been established:

- Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
 - Initial Assessment and Notification of Outage;
 - Activation of the Plan;
 - Fail over to the Disaster Recovery environment;
 - Mitigation;
 - Recovery and Reconstitution phase to ensure that PRESM is validated through testing and that normal operations are resumed.
- Identify the activities, resources, and procedures to carry out PRESM processing requirements during prolonged interruptions to normal operations.
- Assign responsibilities to designated WDH and HHS Tech Group personnel and provide guidance for recovering PRESM during prolonged periods of interruption to normal operations.
- Ensure coordination with other personnel responsible for HHS Tech Group contingency planning strategies. Ensure coordination with external points of contact and vendors associated with PRESM and execution of this Plan.

HHS Tech Group will conduct an annual test of the BCDRP and submit the Disaster Recovery/Business Continuity Test Report that includes the outcome, corrective action plan, and revisions, if any, to the Agency. The current Plan will be updated according to the findings during annual testing.

1.2 Document Scope

This BCDRP has been developed for PRESM, which is classified as a moderate-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. Procedures in this BCDRP are for moderate-impact systems and designed to recover PRESM within 4 hours. This Plan does not address short-term disruptions lasting less than 4 hours, or loss of data at the on-site facility or the user-desktop levels.

1.3 Document Audience

The audience intended for this document includes:

- Project Leadership Team
- Project Team
- Operations and Maintenance Team



1.4 Constraints and assumptions

The following assumptions were used when developing this BCDRP:

- PRESM has been established as a moderate-impact system, in accordance with FIPS 199.
- Alternate processing sites and off-site storage are required and have been established for this system by HHS Tech Group.
- HHS Tech Group maintain current backups of the system software and data at the off-site storage facility in AWS US-Gov-East region.
- Alternate facility has been established at AWS US-Gov-East and are available if needed for relocation of PRESM Information System.
- Key PRESM personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the PRESM BCDRP.
- Recovery Time Objective (RTO) is 4 hours according to SLA #14 SOW
- Recovery Point Objective (RPO) is 24 hours according to Requirement #149 SOW

The PRESM BCDRP does not apply to the following situations:

- Short lasting outages of PRESM components which are not required fail over to an alternate facility.

2 Business Continuity

2.1 Core business processes

In the table below, for each core business process involved in the PRESM solution provided:

- 1) Identification of potential failures for the process;
- 2) Risk analysis;
- 3) Impact analysis;
- 4) Definition of minimum acceptable levels of service/output.

Table 1: Core business processes risk and impact analysis.

Business Process	Potential Failures	Risk Analysis	Impact Analysis	Contingency	SLA
Provider Enrollment, Revalidation and Provider Self-Service	PRESM web portal is not available due to unpredicted event;	PRESM designed as a highly-available solution. Microservices are redundant across 3 availability zones in AWS GovCloud. AWS managed services with 99.9% uptime are used for	Providers can't perform the business process. Significant impact to providers ability to perform the business process.	Restore PRESM functionality in the main facility if possible in the shortest possible timeframe. Restore PRESM in an alternate facility in another geographical	4 hours



		databases and network components. Risk is low.		region, according to the RTO.	
	HelloSign is down;	HelloSign is one of the industry-leading e-signature solutions and provides 99,93% uptime, which makes a risk low.	Providers are unable to submit enrollments application, CoC and Appeals.	No technical contingency.	
	Stripe is down;	Stripe is one of the industry-leading payment solutions and provides 99,999% uptime. The number of providers that require fee payment is very low. Low risk.	Providers can't pay an enrollment fee and submit an application.	Reconfigure PRESM to use offline payment.	
Provider Enrollment, CoC, Appeals review, approval and denial. Site visit management.	PRESM web portal is not available due to unpredicted event.	PRESM designed as a highly-available solution. Microservices are redundant across 3 availability zones in AWS GovCloud. AWS managed services with 99.9% uptime are used for databases and network	Internal users can't perform the business process.	Restore PRESM functionality in the main facility if possible in the shortest possible timeframe. Restore PRESM in an alternate facility in another geographical region,	4 hours



		components. Risk is low.		according to the RTO.	
	Medversant is down.	Screening is asynchronous due to involved manual processing on the Medversant side. No expectation of near real time processing. So PRESM can tolerate delays up to 24 hours. Risk is low.	Delay in the screening process which causes enrollment approval delays.	No contingency.	
	Call Center's physical site is unsafe or inoperable.	Risk of disaster events such as fire, natural disaster, terrorism, etc. Risk is low.	Call Center agents can't take phone calls and access PRESM web portal. No ability for agents and provider specialists to perform the business process.	Call Center agents and provider specialists work from home until the main Call Center physical site is restored or an alternative business site is provided.	
	Internet connectivity is down in Call Center's physical site.	Internet connectivity is required for Call Center to take calls and work with PRESM. Internet outage risk is relatively high; that is why backup	Call Center agents can't take phone calls and access PRESM web portal. No ability for agents and provider specialists to perform the	Switch to a backup Internet connection using Verizon LTE Business Internet	



		internet connection shall be provided.	business process.		
	Power down in Call Center physical site.	Long-lasting power shutdown is medium risk.	Call Center agents can't take phone calls and access PRESM web portal. No ability for agents and provider specialists to perform the business process.	Office equipped with UPS to lower the impact of short term power outages. In case of a long-lasting power outage, Call Center agents and provider specialists work from home until power is up in Call Center physical site.	
	Communication equipment, printer, laptop issues.	Medium risk.	In case of communication equipment outage Call Center agents can't take calls and use the PRESM web portal.	Backup laptops are available in Call Center site for replacement. Buy replacement printer and communication equipment if needed.	
Provider enrollment support through IVR and Call Center	PRESM web portal is not available due to unpredicted events.	PRESM designed as a highly-available solution. Microservices are redundant across 3 availability zones in AWS GovCloud. AWS managed	Providers can't perform the business process. Significant impact to providers ability to perform the	Restore PRESM functionality in the main facility if possible in the shortest possible timeframe. Restore PRESM in an alternate	4 hours

		services with 99.9% uptime are used for databases and network components. Risk is low.	business process.	facility in another geographical region, according to the RTO.	
	Ameyo IVR system is down.	Ameyo provides disaster recovery with low RTO/RPO and 24/7 support. Risk is low.	Providers can't contact PRESM IVR and Call Center, which limits the ability to receive support.	Ameyo provides a Disaster Recovery facility to support PRESM business continuity.	
	Ameyo Call Center software is down.			When the Call Center software crashed, the agents alerted to take notes in Microsoft Word, allowing for documentation of all calls, which is later entered into the system once it comes back up.	
Process approved provider enrollment financial information documents into WOLFS.	Call Center's physical site is unsafe or inoperable.	Risk of disaster events such as fire, natural disaster, terrorism, etc. Risk is low.	Call Center agents can't take phone calls and access PRESM web portal. No ability for agents and provider specialists to perform the	Call Center agents and provider specialists work from home until the main Call Center physical site is restored or an alternative business site is provided.	2 business days

			business process.		
Incoming documents received, staff site visit documentation, and/or other applicable documentation scanned into the system.	Call Center's physical site is unsafe or inoperable.	Risk of disaster events such as fire, natural disaster, terrorism, etc. Risk is low.	Call Center agents can't take phone calls and access PRESM web portal. No ability for agents and provider specialists to perform the business process.	Call Center agents and provider specialists work from home until the main Call Center physical site is restored or an alternative business site is provided.	95% within 2 business days, 5% within 3 business days
	Scanner, laptop issue.	Low risk.	Call Center agents can't scan documents which impact SLA.	Buy replacement scanner. Backup laptops are available in Call Center for replacement.	

2.2 Contingency Plan Triggers

Please refer to section 3.2.1 Activation Criteria and Procedure for contingency plan triggers.

2.3 Business Continuity Procedures

In case of PRESM web portal outage due to disaster event, there is no alternate manual or technical processing procedures available that allow the business unit to continue some processing of information that would normally be done by the affected system. HHS Tech Group provides cloud base solution designed to minimize the impact on business using high availability, redundancy, and auto-recovery concepts. In case of disaster, PRESM will be restored within 4 hours in the main or alternative facility.

HHS Technology Group's primary business site is our headquarters in Fort Lauderdale, FL. Currently, and due to the COVID-19 pandemic, everyone assigned to our HQ office is working from home (as is our entire company). We will, at some point, return to working from our respective offices, and this, of course includes our FL headquarters personnel. If our primary business site / HQ were to become unsafe or inoperable, our staff would immediately return to working from home. This would be mostly instantaneous, thus complying with the requirement of being fully operational within two (2) business days.

2.4 Business Functions Recovery Plan

In the case of BCDRP activation, HHS Tech Group Call Center resources will participate in BCDRP Team and perform responsibilities described in section 3.1.4 Roles and Responsibilities.

After reconstitution of PRESM after a disaster event, the HHS Tech Group operations team will analyze the impact of the disaster and plan the recovery of business functions. The main challenge after system fail over is to identify which operations are lost since backup time and how to replay all lost business transactions. Depending on the time of the disaster, it can be up to 24 h of data lost. So HHS Tech Group operations team will identify all providers affected by the disaster and plan the outreach to inform that providers need to redo the operations they performed during period of time defined by RPO.

2.5 Communication protocols and process for restoring operations

Please refer to section 3.2.2 Notification for details regarding communication protocols and to section 3.4 Recovery for restoring operations.

3 Disaster Recovery

3.1 Concept of Operations

The Concept of Operations section provides details about PRESM, an overview of the five phases of the BCDRP (Activation and Notification, Recovery, and Reconstitution), and a description of roles and responsibilities of WDH and HHS Tech Group personnel during a contingency activation.

3.1.1 System Description

HHS Tech Group awarded to implement the PRESM module for the WINGS project. HHS Tech Group uses the Discover Your Provider (DyP) Solution to implement PRESM requirements listed in SOW. DyP built as an all-inclusive, modular Provider Services solution to support the enrollment and maintenance of all provider types as well as the needs of internal WDH users. DyP built to be both modular and adaptable to meet state-specific needs and to conform to the guidance released by the Centers for Medicare and Medicaid Services (CMS) Medicaid Information Technology Architecture (MITA) Seven Standards and Conditions.

The DyP is a Software as a Service (SaaS), COTS solution built to include:

1. Holistic provider support with wide-ranging functionality through the Provider Portal to include:
 - a. Provider enrollment
 - b. Provider self-service
 - c. Support for additional functionality
2. Backend, administrative user support through the Internal User Portal which enables Agency staff and other HHS Tech Group support users to:
 - a. Review, verify and approve provider submitted information
 - b. Manage the entire application and approval process
 - c. Perform a range of support functions to create efficiencies across traditional workflows
3. Best practices for modularity
4. Design principles for adaptability, ease of use, and interoperability
5. A modern, web-based user experience
6. Self-service functions 24/7/365

7. Adherence to industry regulations, including guidance from CMS, the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Americans with Disabilities Act (ADA) 508 Accessibility Standards

The software system resides within the Amazon AWS GovCloud West region datacenter (Platform-as-a-Service). AWS GovCloud platform maintains compliance with NIST, HIPAA, HITRUST CSF, ITAR, FedRAMP, DoD SRG IL 2, 3,4, and 5, ISO 27001, PCI DSS Level 1, and SOC 2. PRESM components are deployed with high-availability across three availability zones and relying on AWS managed services for network and security functionality. PRESM components are packaged as Docker containers and deployed to the Kubernetes cluster, which provides self-healing capabilities for components. Application components are separated from databases using VPCs for better control and security. Multi-account landing zone architecture with AWS Organizations service is used to separate service based on the least access principle. Multi-availability zone architecture provides redundancy across 3 different data centers, which reduces the possibility of a complete outage. In the case of full regional outage of 3 data centers in the West region, which is extremely unlikely, PRESM will be restored from backups in the East region.

In the diagram below depicted the infrastructure architecture of PRESM Production Environment in AWS GovCloud.

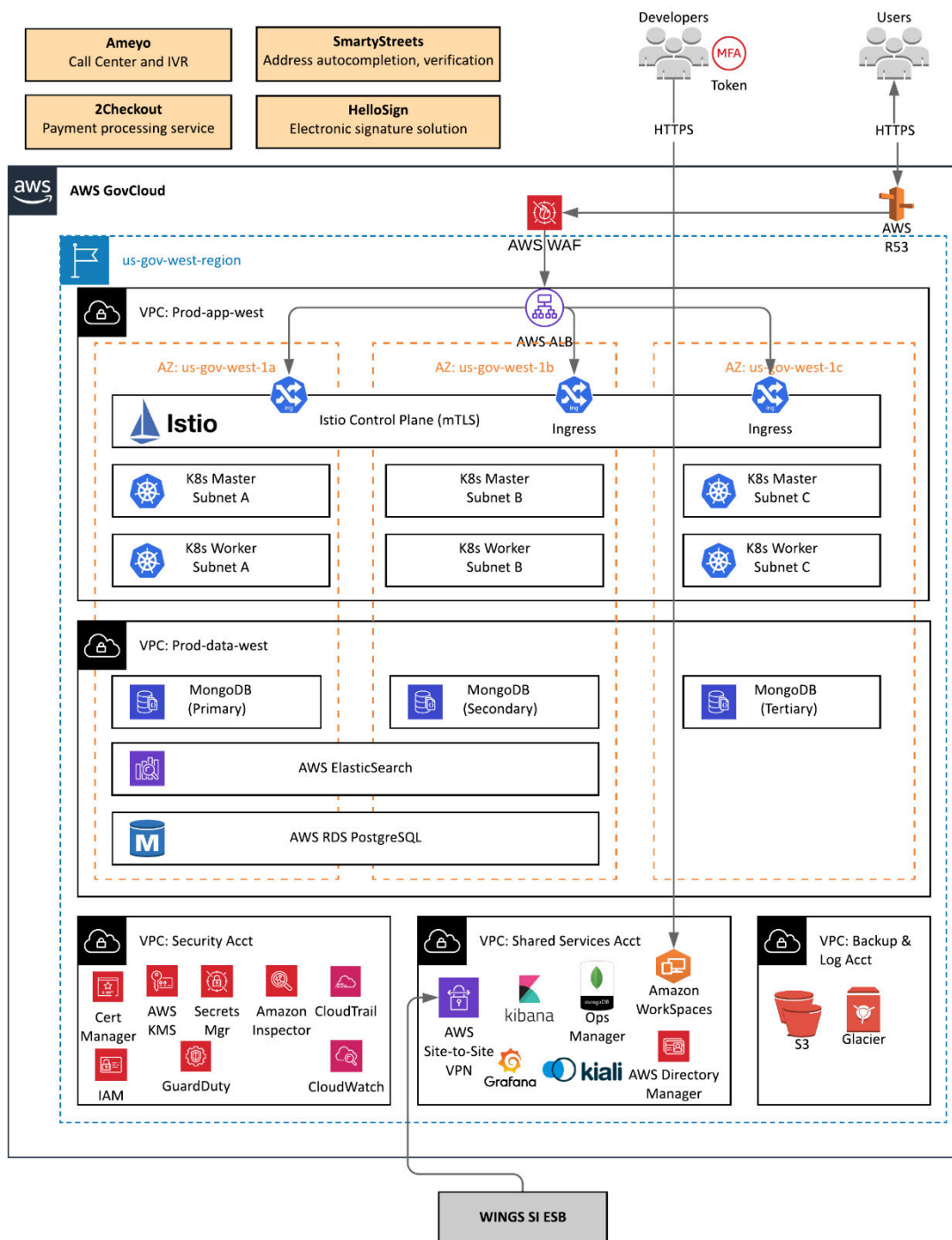


Figure 1. System hardware/software architecture diagram

The diagram below provided high-level view of PRESM operations environment, including physical infrastructure in the HHS Tech Group Call Center office in [REDACTED] and cloud infrastructure, which supports PRESM business processes.

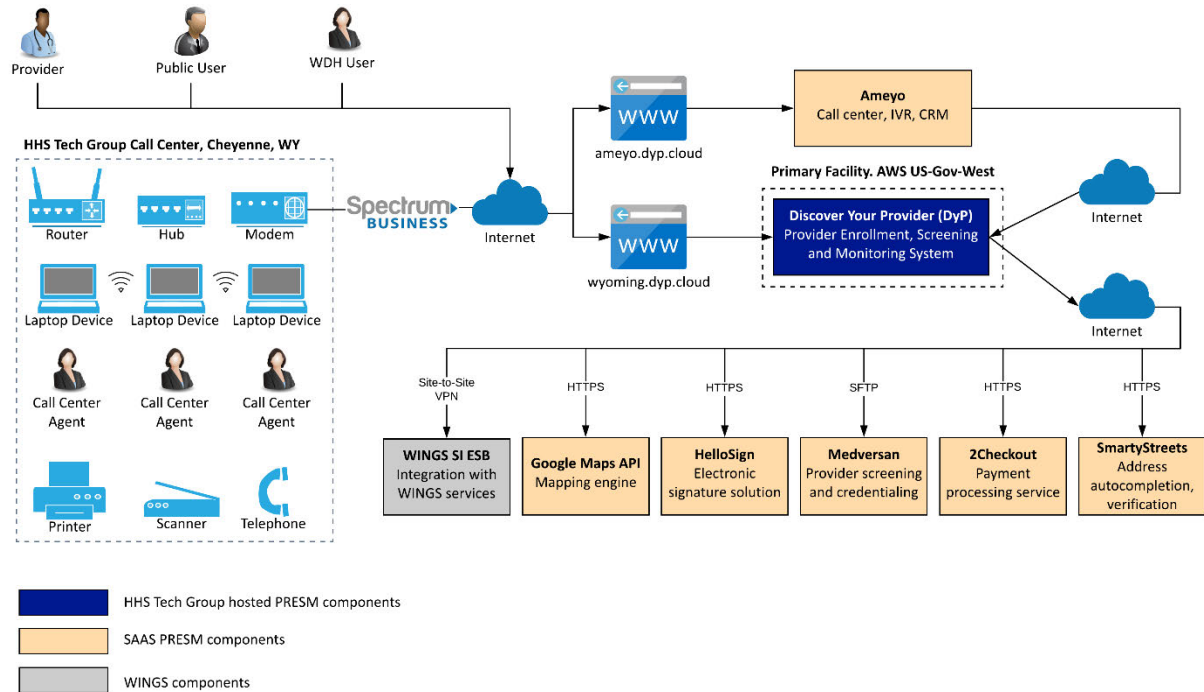


Figure 2. Business as Usual State of PRESM

The next diagram demonstrates how the operational environment looks like in case of a disaster event. Call Center operations require power and Internet connection to perform responsibilities. HHS Tech Group provides main Internet connectivity for Call Center through Spectrum Business cable internet. In case of an internet outage, HHS Tech Group provides failover internet connection through Verizon LTE Business Internet. Call Center is equipped with UPS to maintain power in case of interruption. In the case of a long-lasting blackout, PRESM call center agents can work from home. In the case of disaster events, PRESM Information System will be restored in a disaster recovery facility in the AWS GovCloud East region.

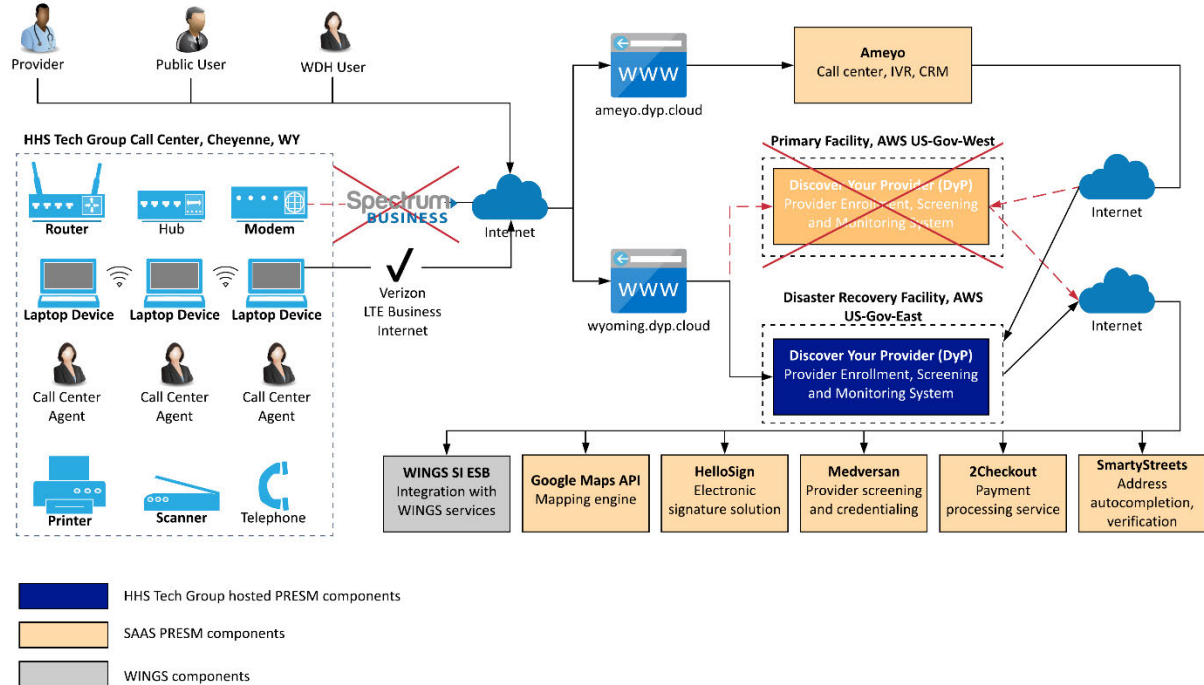


Figure 3. Disaster Recovery State of PRESM

For more information about PRESM system design and solution architecture, please refer to System Design Document, Solution Architecture Document, System Security Plan and Technical Documentation.

3.1.2 Backup Plan, procedures, and schedules

PRESM is hosted in AWS GovCloud US-Gov-West region. As a backup facility for PRESM is used AWS GovCloud US-Gov-East region.

HHS Tech Group uses automated processes to satisfy backup requirements. According to the SOW requirement #149 PRESM configured to use the following backup policies:

1. Daily incremental backups with retention of sixty-one (61) days;
2. Weekly incremental backups with retention of twelve (12) weeks;
3. Monthly full backups with retention of eighteen (18) months;
4. Annual full backups with retention of seven (7) years;

Automated backup is configured to run in non-business hours between 5 and 6 am MST to minimize the impact on the system performance.

HHS Tech Group uses a set of tools to implement an automated backup policy for different components of the Solution. AWS Backup is used for RDS, EC2 and EBS backup. AWS Backup doesn't support backup of AWS Elasticsearch Service; that is why we are using Lambda function and Curator API to automate backup of Elasticsearch indexes to S3 buckets. For Kubernetes cluster backup and restore, we are using [Velero](#), which allows us to automate backup of Kubernetes resources to S3, including persistent volumes. MongoDB

provides Ops Manager console, which allows automating backups of the database to S3. All listed tools provide automated backup schedules, retention management, and lifecycle management, removing the need for manual processes. Highly durable AWS S3 storage with cross-region replication is used for all backups, which allows restoring services to another region when needed. S3 backup buckets are replicated across regions to make sure that snapshots are available in case of complete region outage.

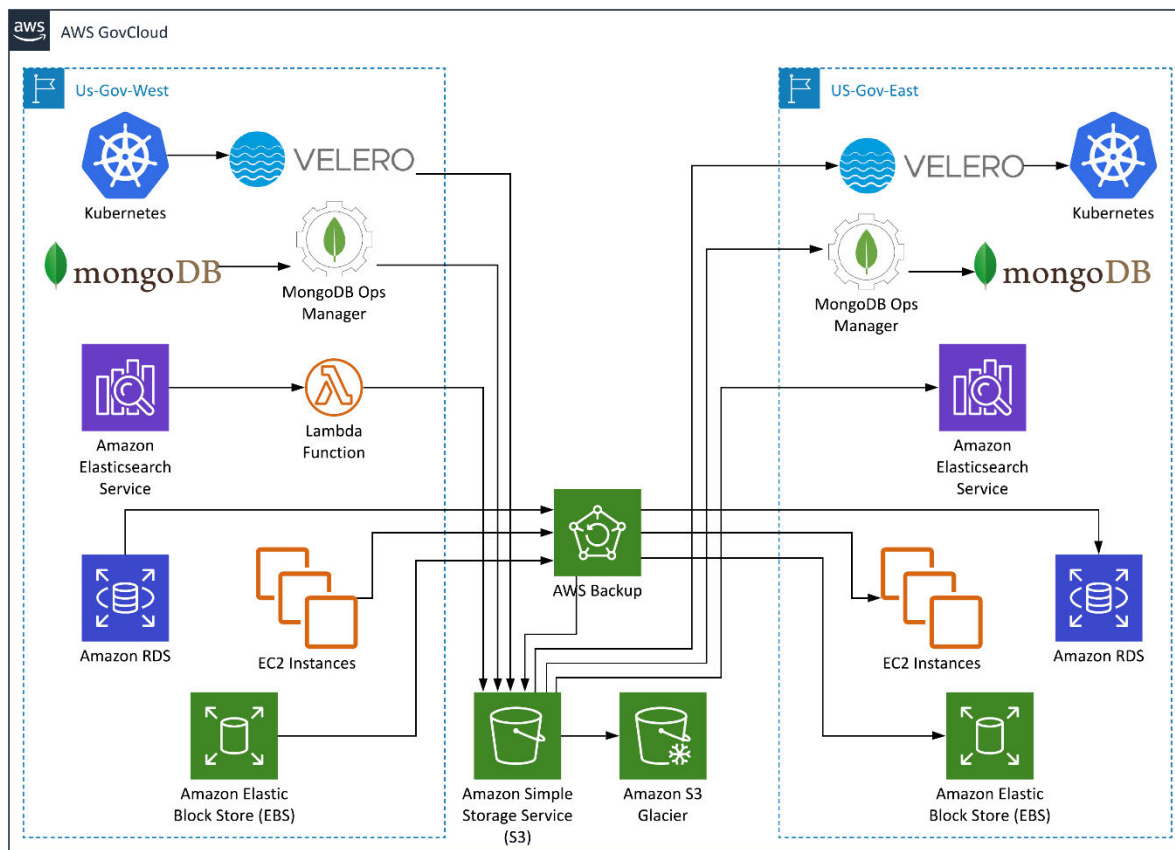


Figure 4. PRESM backup architecture

Backups are useful for unit recovery of failed service such as databases or Kubernetes cluster. But when it comes to disaster events, which causes a large number of services to fail and the timeline for recovery is short, restoration of all services from backup can be time-consuming. To speed up the Disaster Recovery timeline and satisfy RTO of 4 hours, we are using the AWS [CloudEndure](#) disaster recovery solution. Unlike snapshot-based solutions, CloudEndure performs block-level replication, which enables minimal Recovery Point Objectives (RPOs) for all applications and databases running on supported operating systems. CloudEndure's replication process doesn't impact performance or require a reboot. HHS Tech Group uses CloudEndure in combination with traditional backup/restore tools to expedite the recovery process.

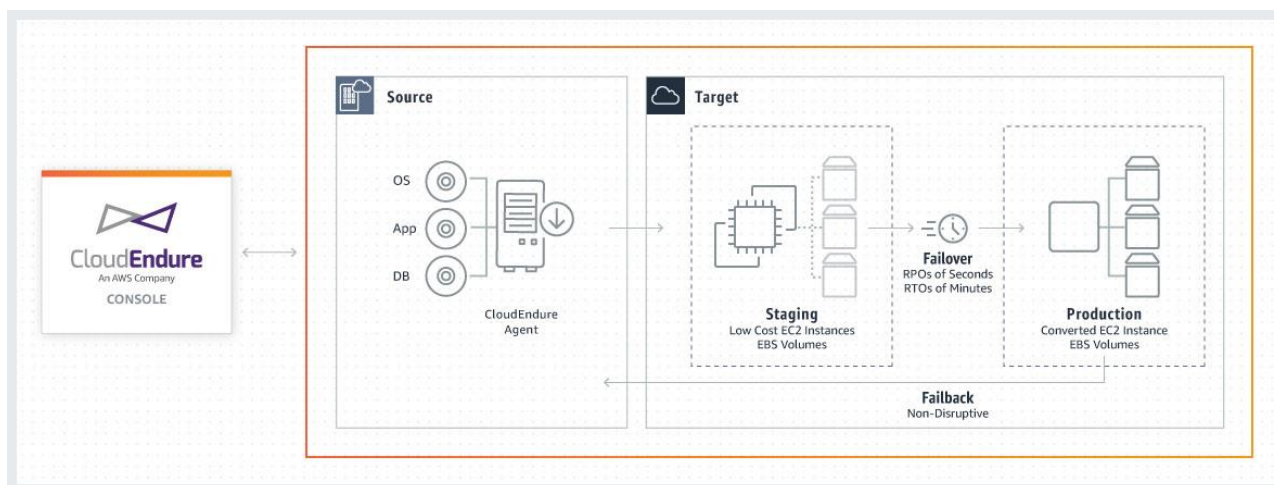


Figure 5. CloudEndure disaster recovery solution

3.1.3 Overview of Five Phases

This BCDRP has been developed to recover and reconstitute the PRESM using a five-phased approach. This approach ensures that system recovery and reconstitution efforts are performed in a methodical sequence to maximize the effectiveness of the recovery and reconstitution efforts and minimize system outage time due to errors and omissions.

The five system recovery phases are:

Initial Assessment and Notification of Outage - System owners and users are notified of a possible long-term outage, and a thorough outage assessment is performed for the system. Information from the outage assessment is presented to system owners and may be used to modify recovery procedures specific to the cause of the outage.

Activation of the Plan – Activation of the BCDRP occurs after a disruption or outage that may reasonably extend beyond the RTO established for a system. The outage event may result in severe damage to the facility that houses the system, severe damage or loss of equipment, or other damage that typically results in a long-term loss.

Fail over to the Disaster Recovery environment – The fail over phase details the activities and procedures for the recovery of the affected system to disaster recovery environment. Activities and procedures are written at a level that an appropriately skilled technician can recover the system without intimate system knowledge. This phase includes notification and awareness escalation procedures for communication of recovery status to system owners and users.

Mitigation – Mitigation phase includes activities related to liquidation of damages caused by disaster in the main facility and preparation of the main facility to the reconstitution.

Reconstitution – The Reconstitution phase defines the actions taken to test and validate system capability and functionality at the original or new permanent location. This phase consists of two major activities: validating successful reconstitution and deactivation of the Plan.



During validation, the system is tested and validated as operational prior to returning operation to its normal state. Validation procedures include functionality or regression testing, concurrent processing, and/or data validation. The system is declared recovered and operational by system owners upon successful completion of validation testing.

Deactivation includes activities to notify users of system operational status. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, and readying resources for any future events.

3.1.4 Roles and Responsibilities

The BCDRP Team will perform the following functions:

- Initiate and implement the BCDRP within the predefined contractual timeline
- Institute predefined roles and responsibilities for all contingency types
- Inform users of policies and procedures
- Abide by the published security policies

The next figure illustrates the HHS Tech Group BCDRP Team structure.

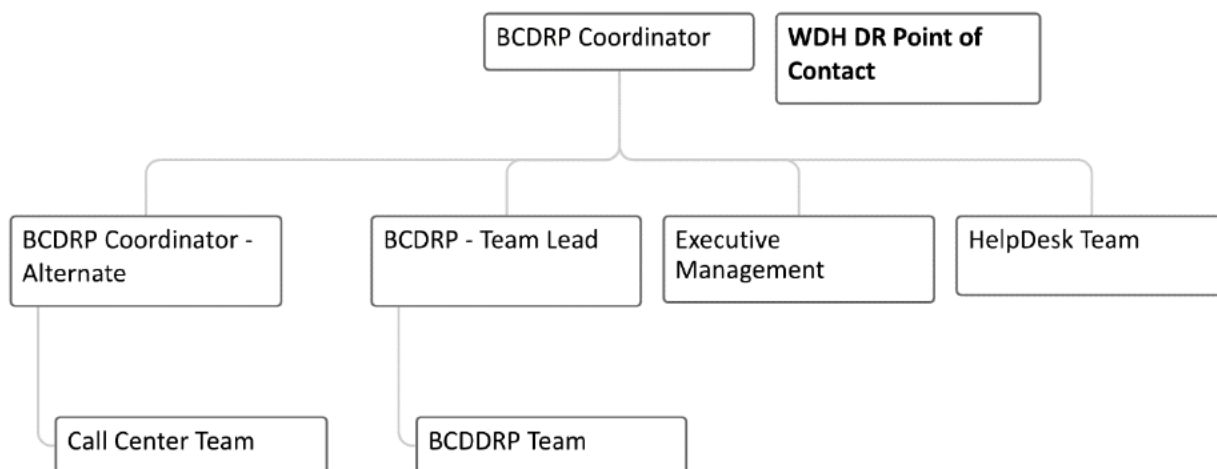


Figure 6. PRESM Disaster Recovery Team structure

Please refer to Appendix C for contact information for key personnel involved in the BCDRP Team.

The table below lists designees for each BCDRP Team function. This table will be updated with names, titles, and contact information as it becomes available.

Table 2: Assigned BCDRP Function / Assignees

DRT Function	Assignee(s)	Assignee Name
	WDH PRESM Contract Manager	Sheree Nall

WDH DR Point of Contact (POC)	WDH PRESM Project Manager	Kaitlyn Wilson
	WDH PRESM Technical Manager	Barbara Grofe
BCDRP Coordinator	HHS Tech Group Operations Manager	Richard Hammontree
Executive Management	HHS Tech Group executive leadership	Thomas Swider, Faiyaz Shikari
BCDRP Coordinator - Alternate	HHS Tech Group Call Center Lead	Kelly Miller
BCDRP – Team Lead	HHS Tech Group Technical Manager	Leonid Marushevskyi

The functions, roles, and responsibilities of the following individuals and teams are summarized below.

- **WDH DR Point of Contact (POC)** – are designated contact persons from WDH which are included in all disaster recovery and business continuity communication and decision making in scope of BCDRP.
- **BCDRP Coordinator** – In critical downtime situations, or in a natural disaster, the BCDRP Coordinator or designee will take primary responsibility of all communications to the WDH DR POC, Executive Management, and BCDRP Team. The BCDRP Coordinator will consult with the WDH DR POCs, technical and operations groups, technical and management teams, providing all pertinent updates to the POC. All updates will be communicated immediately to all affected members. The BCDRP Coordinator will lead and schedule all meetings, facilitating and presenting all pertinent facts as to the operational condition of the system or affected area. The BCDRP Coordinator will normally schedule these meetings as conference calls unless circumstances require the need for in-person meetings. The BCDRP Coordinator will ensure that all meeting minutes are captured, reviewed for accuracy, and posted to the PRESM Securisync repository.
- **BCDRP Coordinator - Alternate** – Backup person who plays the role of BCDRP Coordinator in case of the main assignee is not available to participate.
- **BCDRP – Team Lead** – Person who leads the BCDRP Team. Participate in to provide technical expertise and communicate technical details to the rest of the team and POC.
- **BCDRP Team** – Cross-functional technical support and operations team responsible for PRESM reconstitution in case of disaster. During escalated calls or a critical systems failure, the BCDRP Team members will be actively engaged to find an immediate resolution. This team will stay engaged until the failure has been corrected, and the situation has been resolved. This will be a parallel process to the initiation of the BCDRP itself. The HHS Tech Group will ensure that all required network communications have switched over and are functioning correctly. Upon notification of a problem issue, the HHS Tech Group BCDRP Team will assess the issue, prioritize, assign resources, and begin problem resolution. This may include any of the assigned duties or tasks leading up to a DR switchover. At all times, the BCDRP Team will make every effort to address issues in a timely manner. This could include issues that are compounded by network problems and may require coordination between various groups for resolution. Other PRESM network issues involving technical system issues will require the BCDRP Team to remain engaged while working with the HHS Tech Group HelpDesk Team.

- **HelpDesk Team** – Team is responsible to work with vendors and Call Center Team in regards to internet and phone connectivity, hardware issues.
- **Call Center Team** – Team is responsible for business continuity, information support, and functional validation of the Solution after recovery.

3.2 Activation and Notification

The Activation and Notification Phase defines initial actions taken once a PRESM disruption has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, conduct an outage assessment, and activate the BCDRP. At the completion of the Activation and Notification Phase, PRESM BCDRP staff will be prepared to perform recovery measures to restore system functions.

3.2.1 Activation Criteria and Procedure

The PRESM BCDRP may be activated if one or more of the following criteria are met:

1. The type of outage indicates PRESM web portal will be down for more than 4 hours;
2. Primary business site in [REDACTED] becomes unsafe or inoperable;
3. Other criteria, as appropriate.

3.2.2 Notification

In the event a system failure occurs, the BCDRP will be invoked via the following communications/escalations. This process is in addition to the normal HHS Tech Group technical/management escalation process, which would happen on any system outage condition (break-fix maintenance).

- The HHS Tech Group BCDRP Coordinator shall immediately send out notifications via email and phone communications to WDH DR POC, BCDRP Coordinator – Alternative, BCDRP Team Lead calling for a meeting be held immediately via conference call.
 - At the BCDRP initiation meeting, the BCDRP Coordinator will brief everyone on the situation, indicating which measures can or will be taken.
 - Upon agreement by WDH and HHS Tech Group, the BCDRP is initiated.
 - Respective BCDRP members will perform their designated functions.
 - Direct communications with the respective teams will be coordinated through the BCDRP Coordinator.
 - Notification to System Integrator, Deloitte support team (ushealthinteractivemoteam@deloitte.com), will be sent by BCDRP Coordinator to inform about PRESM availability interruption.
 - The HHS Tech Group BCDRP Team will handle all configuration changes.
 - Minimally every four (1) hours, the BCDRP Coordinator will brief the POC. These updates will come in one of two forms:
 - A hosted call-in conference call meeting subsequent to the initial meeting
 - Email updates

Communications updates will continue until the BCDRP implementation move has been completed from primary to the alternate site and PRESM reconstituted.

- Email updates will follow the following format:



- Problem or Issue
 - Action item (Tasks to complete)
 - ETA/Completion
 - Impact or result of the situation at hand
- Upon completion of corrective measures to repair the inactive site, the transition back to operational status will begin with HHS Tech Group providing continued status and updates until completion.
 - Upon completion of this transition, the BCDRP Coordinator will provide a Root Cause Analysis documenting the problem, cause, correction, and how it may be prevented in the future.

3.2.3 Notification – External

During a system outage, it is also critical to notify the PRESM end-users of the system. PRESM web portal shall show that PRESM is temporary down for maintenance with a timeline for restoration of the service. BCDRP Coordinator informs Call Center agents about the status of recovery and Call Center Lead coordinates information support of users who call to the PRESM IVR line.

3.3 Outage Assessment

Following notification, a thorough outage assessment is necessary to determine the extent of the disruption, any damage, and expected recovery time. This outage assessment is conducted by HHS Tech Group PRESM BCDRP Team. Assessment results are provided to the BCDRP Coordinator to assist in the coordination of the recovery of PRESM.

3.4 Recovery

The Recovery Phase provides formal recovery operations that begin after the BCDRP has been activated, outage assessments have been completed, personnel have been notified, and appropriate teams have been mobilized. Recovery Phase activities focus on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or an alternate location. At the completion of the Recovery Phase, PRESM will be functional and capable of performing the functions identified in Section 3.1.1 of this Plan.

3.4.1 Sequence of Recovery Activities

The following activities occur during recovery of PRESM:

1. Identify the required resources to perform recovery procedures;
2. Validate backups availability;
3. Recover AWS infrastructure services in another AWS region;
4. Recover PRESM components from backups
5. Reconfigure DNS
6. Validate the restored system

3.4.2 Recovery Procedures

The following procedures are provided for the recovery of PRESM at an alternate site in AWS GovCloud East region. Recovery procedures should be executed in the sequence presented to maintain an efficient recovery effort.

Table 3: Recovery Procedure



#	Recovery Steps	Responsibility
1	Reconfigure Rout53 PRESM web portal [REDACTED] domain to maintenance page to prevent users from using broken system.	BCDRP Team
2	Restore cloud infrastructure Use PRESM Prod Recovery Plan in CloudEndure to restore AWS infrastructure in disaster recovery facility in AWS US-Gov-East region. When completed CloudEndure will restore all EC2, EBS, VPC, Subnets, ELB and security groups.	BCDRP Team
Restore databases		
3	Restore RDS PostgreSQL database from backup in S3 to AWS GovCloud East region using AWS Backup service.	BCDRP Team
4	Restore Elasticsearch from backup in S3 to AWS GovCloud East region.	BCDRP Team
5	Restore AWS RDS MySQL database from backup in S3 to AWS GovCloud East region using AWS Backup service.	BCDRP Team
6	Reconfigure DNS for MongoDB restored by CloudEndure into US-Gov-East in step 2	BCDRP Team
7	Reconfigure Rout53 for Sisense restored by CloudEndure into US-Gov-East in step 2	BCDRP Team
Restore Applications cluster		
8	Install Kubernetes cluster in AWS US-Gov-East using kops.	BCDRP Team
9	Setup network peering between VPCs. Establish network connectivity between data and Kubernetes VPCs.	BCDRP Team
10	Restore PRESM applications deployed to Kubernetes cluster. Use Velero to restore Kubernetes cluster state from backup in S3.	BCDRP Team
Configure DNS and load balancing		
11	Configure DyP Load Balancer.	BCDRP Team
12	Reconfigure DNC and Load Balancer for Help Center.	BCDRP Team
13	Reconfigure DNS and Load Balancer for CSDN Content.	BCDRP Team
14	Change deployment configuration and redeploy applications.	BCDRP Team
15	Reconfigure and validate site-to-site VPN to SI ESB network from AWS US-Gov-East.	BCDRP Team
Reconfigure applications		
16	Reconfigure DyP and Content to use new databases.	BCDRP Team

17	Reconfigure Rout53 PRESM web portal [REDACTED] back to production ELB in AWS GovCloud East region.	BCDRP Team
----	--	------------

Detailed keystroke-level procedures will be provided after Disaster Recovery Business Continuity Testing is performed and will be attached to the current Plan as Appendix D. Detailed recovery procedures.

3.4.3 Recovery Escalation Notices/Awareness

During the recovery process, BCDRP Team Lead performs an assessment of the progress and provides notification every 1 hour to BCDRP Coordinator in the form of an email with information about recovery status and problem escalation to leadership and WDH. BCDRP Coordinator is responsible for propagating recovery status information WDH DR POC, and Executive Management.

3.5 Reconstitution

Reconstitution is the process by which recovery activities are completed, and normal system operations are resumed. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements. A determination must be made on whether the system has undergone significant change and will require reassessment and reauthorization. The phase consists of two major activities: validating successful reconstitution and deactivation of the Plan.

3.5.1 Validation Data Testing

Validation data testing is the process of testing and validating data to ensure that data files or databases have been recovered entirely at the permanent location. Database Administrator shall perform the following procedures to determine that the data is complete and current to the last available backup:

1. Connect to MongoDB and validate that data in providermgmt database correlate with the backup date. Document date for most recent records in providerData and runtimeApplicatins collections.
2. Connect to Elasticsearch and validate the latest dates for objects in audit_events_provider and audit_events_medicaid indexes. Check that dates are in alignment with Elasticsearch backup date.

Additional data validation will be performed in the scope of System Validation Test Plan, which is outlined in Appendix F.

3.5.2 Validation Functionality Testing

Validation functionality testing is the process of verifying that recovered PRESM functionality has been tested, and the system is ready to return to normal operations. Functional validation will be performed by Call Center Team using System Validation Test Plan in Appendix F.

3.5.3 Recovery Declaration

Upon successfully completing testing and validation, the BCDRP Coordinator will formally declare recovery efforts complete, and that PRESM is in normal operations. PRESM business and technical POCs will be notified of the declaration by the BCDRP Coordinator.

3.5.4 Notification (users)

Upon return to normal system operations, the maintenance page will be removed from PRESM web portal, and users will be able to use the system as usual.

3.5.5 Cleanup

Once the Primary site is up, HHS Tech Group and WDH will collectively decide the failback date and time. This means the system will be put to normal processing. All the agency connections and interfaces will be switched to the primary site. The system will be back to the state before the disaster. The maintenance window will be requested 5 days in advance and approved with WDH to perform failback.

3.5.6 Data Backup

As soon as reasonable following recovery, PRESM should be fully backed up and a new copy of the current operational system stored for future recovery efforts. This full backup is then kept with other system backups.

The procedures for conducting a full system backup are:

1. Perform a manual backup of RDS PostgreSQL in US-Gov-East using AWS Backup service;
2. Perform a manual backup of RDS MySQL in US-Gov-East using AWS Backup service;
3. Perform a manual backup of Kubernetes cluster in US-Gov-East using Velero;
4. Perform a manual backup of MongoDB database in US-Gov-East using MongoDB OpsManager;
5. Perform a manual backup of all EC2 instances in US-Gov-East using AWS Backup service;
6. Reconfigure CloudEndure to replicate data for protected instances from US-Gov-East to US-Gov-West region for future;
7. Configure automated backup according to backup Plan in section 3.1.2.

All backups should be stored in AWS S3. The described full backup procedure will be performed by BCDRP Team.

3.5.7 Event Documentation

It is important that all recovery events be well-documented, including actions taken and problems encountered during the recovery and reconstitution effort, and lessons learned for inclusion and update to this BCDRP. It is the responsibility of each BCDRP team to document their actions during the recovery and reconstitution effort and to provide that documentation to the BCDRP Coordinator.

Types of documentation that should be generated and collected after a contingency activation include:

- Activity logs (including recovery steps performed and by whom, the time the steps were initiated and completed, and any problems or concerns encountered while executing activities);
- Functionality and data testing results;
- Lessons learned documentation; and
- After Action Report.

3.5.8 Deactivation

Once all activities have been completed, and documentation has been updated, the BCDRP Coordinator will formally deactivate the BCDRP recovery and reconstitution effort. Notification of this declaration will be provided to all business and technical POCs.



Appendix A. Definition of Terms and Acronyms

Term	Definition
ALB	Application Load Balancer
API	Application programming interfaces
AWS	Amazon Web Services
BC	Business Continuity
BCP	Business Continuity Plan
BCDRP	Business Continuity and Disaster Recovery Plan
BIA	Business Impact Analysis
BRP	Business Resumption Plan
CMP	Change Management Plan
CMS	Centers for Medicare and Medicaid Services
COTS	Commercial-Off-The-Shelf
CP	Contingency Plan
DNS	Domain Name System
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DRT	Disaster Recovery Team
DyP	Discover Your Provider
EBS	Elastic Block Store
EC2	Elastic Computer Cloud
ELB	Elastic Load Balancing
ESB	Enterprise Service Bus
FIPS	Federal Information Processing Standards
IAM	Identity and access management
IR	Incidence Response
MTD	Maximum Tolerable Downtime
OS	Operating system
PaaS	Platform as a service
PRESM	Provider Enrollment, Screening & Monitoring
POC	Point of Contact
RDS	Relational Database Service
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SDD	System Design Document
SOW	Statement of Work
VPC	Virtual Private Clouds
VPN	Virtual private network



WRT	Work Recovery Time
UPS	Uninterruptible Power Supply



Appendix B. Referenced Documents

Please make sure that you are logged into the Securisync before using links in the table below.

Document Name	Document Location and/or URL	Issuance Date
Change Management Plan	Securisync folder	11/08/2019
Solution Architecture Document	Securisync folder	01/13/2020
Master Test Plan	Securisync folder	03/16/2020
System Design Document	Securisync folder	04/15/2020
Technical Documentation	Securisync folder	03/11/2020
Project Work Plan	Securisync folder	12/20/2019
System Security Plan	Securisync folder	04/01/2020
Requirements Traceability Matrix	Securisync folder	01/15/2020

**Appendix C. Personnel Contact List**

Contact information for each person with a role or responsibility for the activation or implementation of the BC/DR. Contact information, such as emergency phone numbers, contact names, contact numbers, and contractual response and on-site times, should be included.

PRESM BCDR Key Personnel	
BCDRP Coordinator	
Richard Hammontree, Operations Manager	Phone: (503) 277-8997 Email: richard.hammontree@HHS Tech Group.com Hours: 8.00 am – 5.00 pm Location: remote
BCDRP Coordinator – Alternate	
Kelly Miller, Call Center Lead	Phone: (307) 316-0051 Email: kelly.miller@HHS Tech Group.com Hours: 8.00 am – 5.00 pm Location: on-site
BCDRP Team – Team Lead	
Leonid Marushevskiy, Technical Manager	Phone: (573) 462-9601 Email: leonid.marushevskiy@HHS Tech Group.com Hours: 8.00 am – 5.00 pm Location: remote
HelpDesk Team	Email: HelpDesk@HHS Tech Group.com Hours: 8.00 am – 5.00 pm

Appendix D. Vendor Contact List

Service	Vendor	Contacts
Office Management	Investors Properties, LLC	Mark Lockwood, Office Manager Work: (970) 226-2600 #2, Mobile: (970) 539-2338 Email: mark@investors-usa.com Hours: business hours
Internet	Spectrum Business, Charter Communications	https://www.spectrumbusiness.net/support Phone: (800) 314-7195 Alternative Phone: (877) 313-2549 Hours: business hours
Failover Internet	Verizon LTE Business Internet	https://www.spectrumbusiness.net/support Phone: (800) 837-4966 Alternative Phone: (877) 297-7816 Hours: business hours
Phone connection	Mitel	Phone: (800) 722-1301 Hours: business hours
Gas and Electrics	Black Hills Energy	Phone: (800) 694-8989 Hours: business hours
Call Center Software	Ameyo	Support Portal URL: https://ameyo.force.com Phone: +1-272.422.0712 Email: apc@ameyo.com Contact Person Name: Mohil Gupta (Account Manager)
Screening Service	Medversant	Phone: (213) 291-6139 Email: support@medversant.com Hours: Business hours
Reporting module	Sisense	Support portal: https://support.sisense.com/hc/en-us/requests/new Hours: 24/7
Database Support	MongoDB	Support Portal: https://support.mongodb.com/welcome Email: support-operations@mongodb.com Hours: 24/7
Cloud Infrastructure Support	Amazon Web Services	Support portal: https://console.amazonaws-us-gov.com/support/home?# Hours: 24/7
Address Validation Service	SmartyStreets	Support portal: https://smartystreets.com/contact-support Hours: 24/7 Phone: (801) 877-5778 After Hours Emergency Phone: (801) 960-2067 Email: support@smartystreets.com

On-line Payment Service	2Checkout	Support portal: https://www.2checkout.com/merchant-support/ Hours: 24/7
Electronic Signature Service	HelloSign	Support portal: https://faq.hellosign.com/hc/en-us/requests/new Email: support@hellosign.com Hours: 24/7
WINGS System Integrator	US Health Interactive M&O Team	Email: ushealthinteractivemoteam@deloitte.com



Appendix E. Detailed recovery procedures

Information will be provided in next versions of this document after the Disaster Recovery Business Continuity Test will be performed and documented.



Appendix F. System Validation Test Plan

Validation steps designed in such a way that it can be done by HHS Tech Group Call Center staff without special testing skills, in a time span of 5-10 minutes, and covers most of PRESM functionality. System Validation Test Plan shall be executed by multiple team members in parallel to speed up the testing timeline.

Once the system has been recovered, the following steps will be performed to validate system data and functionality:

#	Procedure	Expected Results	Actual Results	Successful?	Performed by
1. Technical Validation (required to be done before next sections)					
1.1	Validate EC2 instances with PRESM components in AWS US-Gov-East region.	All EC2 instances in AWS US-Gov-East region are up and in healthy state.			BCDRP Team
1.2	Validate application containers in Kubernetes cluster in AWS US-Gov-East region.	All application containers in Kubernetes cluster in AWS US-Gov-East are up.			BCDRP Team
1.3	Validate Site-to-site VPN with SI, Deloitte. Validate connectivity to SI Movelt SFTP from AWS US-Gov-East region.	Site-to-site VPN between AWS US-Gov-East and SI, Deloitte is up and connectivity can be established with SI Movelt SFTP from AWS US-Gov-East.			BCDRP Team
1.4	Validate connectivity to Medversant SFTP server from AWS US-Gov-East region.	Connectivity with Medversant SFTP from AWS US-Gov-East region can be established.			BCDRP Team
1.5	Review application logs to identify any errors which needs to be addressed.	Application logs has no unexpected errors.			BCDRP Team



2. Provider Functions					
2.1	Register new provider user.	Registration is successful. Registration email received. User able to confirm registration.			Call Center Team
2.2	Login into DyP using newly registered provider.	Login is successful and user can see page with enrollment types selection.			Call Center Team
2.3	Create individual enrollment and go through all enrollment steps without finishing the enrollment. Delete enrollment after the test.	Address autocompletion and validation through SmartyStreets is working. NPI check is working. HelloSign interface is invoked (don't need to finish signing).			Call Center Team
2.4	Log off the system.	User successfully logged off.			Call Center Team
3. Internal User Functions					
3.1	Login to DyP using Internal user account with System Admin role.	User successfully logged in to the system and main menu shows.			Call Center Team
3.2	Navigate to Provider menu and perform provider search.	Search returns list of providers without any filters. Number of providers is close to the number of before the outage minus number of providers lost due to outage since last backup (up to 24 hours of data). Search criteria allow to filter provider list.			Call Center Team



3.3	Navigate to Enrollment menu and perform enrollments search.	Search returns list of enrollments without any filters. Number of enrollments is close to the number before the outage minus number of enrollments lost due to outage since last backup (up to 24 hours of data). Search criteria allow to filter enrollment list.			Call Center Team
3.4	Navigate to CoC menu and perform CoC search.	Search returns list of CoC without any filters. Number of CoC is close to the number before the outage minus number of CoC lost due to outage since last backup (up to 24 hours of data). Search criteria allow to filter CoC list.			Call Center Team
3.5	Navigate to Appeal menu and perform appeals search.	Search returns list of appeals without any filters. Number of appeals is close to the number before the outage minus number of appeals lost due to outage since last backup (up to 24 hours of data). Search criteria allow to filter appeals list.			Call Center Team
3.6	Navigate to Audit menu and perform audit events search.	Search returns list of audit without any filters. Search criteria allow to filter audit events list.			Call Center Team
3.7	Navigate to Reports -> Canned and Ad Hoc menu and test reports.	Sisense embedded interface shows. All reports show data.			Call Center Team



3.8	Navigate to Site Visit menu and perform site visits search.	Search returns list of site visits without any filters. Number of site visits is close to the number before the outage minus number of site visits lost due to outage since last backup (up to 24 hours of data). Search criteria allow to filter site visit list.			Call Center Team
3.9	Navigate to Help Center menu and smoke test Help Center functionality.	Help Center interface shows. Search is working. Navigation menu is working.			Call Center Team
3.10	Navigate to Documents menu and smoke test ECM (Content).	Content interface shows in embedded iframe. Internal user can see files and search for files. User able to download existing file. User able to upload and delete new file. All folders are in place and accessible.			Call Center Team
3.11	Navigate to System Options and validate configuration against Golden Configuration Spreadsheet.	System Options configured according to the Golden Configuration Spreadsheet.			Call Center Team
3.12	Log off the system.	User successfully logged off.			Call Center Team
4. IVR and Call Center functionality					
4.1	Call to PRESM IVR phone line and validate IVR functionality.	IVR system respond and functionality is working. User one of existing providers to validate IVR functionality.			Call Center Team



4.2	Login to Ameyo Call Center portal and validate functionality.	Ameyo Call Center portal perform as expected. Integration between Ameyo and DyP is working. Validate that Ameyo shows embedded DyP interface with information about providers. Embedded Help Center interface in Ameyo is working.			Call Center Team
4.3	Validate Ameyo reporting functionality.	Reports are working as expected.			Call Center Team
5. Public Landing Page functionality					
5.1	Navigate to Provider Search menu on the landing page of the PRESM portal.	Provider Search page shows Google map and default to the address of the user. Search functionality is working and providers are visible on the map.			Call Center Team
5.2	Validate that Providers News and Updates show as expected .	Latest news are shown on the landing page. When click on Show All News, user can see all news and updates with history.			Call Center Team