Strafford

Presenting a live 90-minute webinar with interactive Q&A

Healthcare and Ransomware Attacks: Protecting Patient Information, Mitigating Privacy Risks

Determining Reportable Breach, Challenges With Third-Party Vendors

WEDNESDAY, MARCH 17, 2021

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Scott T. Lashway, Partner, Co-Leader Privacy and Data Security Practice Group, **Manatt, Phelps & Phillips, LLP**, Boston

Lindsay B. Nickle, Partner, Vice Chair of the Data Privacy & Cybersecurity Practice, **Lewis Brisbois Bisgaard & Smith, LLP**, Dallas

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

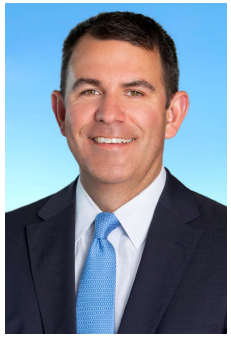
If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

Healthcare and Ransomware Attacks

Presented by Scott Lashway and Lindsay Nickle

Presenters



Scott T. Lashway, Partner
Manatt, Phelps & Phillips, LLP
Boston, Massachusetts
SLashway@manatt.com
617.646.1401

Lindsay B. Nickle, Partner
Lewis Brisbois, LLP
Dallas, Texas
Lindsay.Nickle@lewisbrisbois.com
214.722.7141

Ransomware Attacks – The Most Dynamic and Dangerous Threat

- **Sophisticated Attacks … Increasingly Dangerous**
  - Thorough, persistent & patient reconnaissance
  - Credential stealing Trojans
  - Customized malware to evade anti-virus products
  - Legitimate applications used for malicious purposes
  - Deletion/encryption of backup data
  - Encryption of core applications, networks
- **Attack Monetization … Increasingly Expensive**
  - High value targets
    - MSPs, supply chains, etc.
  - Increasing ransom demands
  - Exfiltration of sensitive data prior to encryption
    - Preliminary posting of sensitive data to leverage ransom payment
  - Extortion for both encrypted & exfiltrated data

Encryption Attacks – Ethics & Notification Obligations

- **Exfiltration of Data … Increasingly Malicious**
  - Data exfiltrated but not posted
  - Data exfiltrated and posted on private ransomware variant site
  - Data exfiltrated and posted on public ransomware variant shaming site
- **Possible Notification Obligations … Increasingly Complex**
  - Data breach notification statutes – to be discussed …
  - Federal sector regulatory notification obligations
    - HIPAA – to consumers and regulator
    - FERPA – to regulator
    - FINRA – to regulator
  - Industry notification obligations
    - PCI DSS – to merchant processor/payment card brands
  - Client contractual notification obligations
  - Ethical obligations
    - Legal vertical

What is HIPAA

- HIPAA stands for “Health Insurance Portability and Accountability Act”
  - Privacy Rule (45 C.F.R. §§164.500-164.534)
  - Security Rule (45 C.F.R. §§164.302-164.318)
  - Breach Notification Rule (45 C.F.R. §§164.400-164.414)
  - Definitions (45 C.F.R. §§160.103)

HIPAA Breach Notification

- The HIPAA Breach Notification Rule
  - Requires Covered Entities and Business Associates to provide notification following a breach of unsecured protected health information.
  - "Breach" is an impermissible use or disclosure of PHI that compromises the security or privacy of PHI.
  - 45 C.F.R. §§164.400-164.414

Definition of PHI

- Generally, PHI (protected health information) is any information in a medical record that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as a diagnosis or treatment.
  - Includes demographic information.
  - Includes information regarding past, present, or future physical or mental health or condition.
  - Includes payment and insurance information.

Definition of PHI (cont.)

- The elements of PHI can be found in the de-identification rule
  - 45 C.F.R. §164.514
  - 18 categories of information
  - The categories of PHI are:
    - Names
    - All geographic subdivisions smaller than a state (i.e. addresses)
    - All elements of dates (except year) directly related to an individual, including DOB, admission or discharge date, and date of death.
    - Telephone numbers
    - Fax numbers

Definition of PHI (cont.)

- Elements (continued)
  - Email addresses
  - Social Security Numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers and serial numbers, including license plate numbers

Definition of PHI (cont.)

- Elements (continued)
  - Device identifiers and serial numbers
  - Web Universal Resource Locators
  - Internet Protocol address numbers
  - Biometric identifiers, including finger and voice prints;
  - Full face photographic images and any comparable images; and
  - Any other unique identifying number, characteristic, or code

Definition of PHI (cont.)

- For the information listed to be considered PHI, it must be found in combination with health condition, health care provision, or health care payment data.
  - https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected.

- The relationship with health information is fundamental. Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to heath data (see above). If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.

Exceptions to HIPAA Breach Definition

- Exceptions to Breach
  - Good faith acquisition by a workforce member.
  - Inadvertent disclosure to another person within the same organization
  - Disclosure of PHI with a good faith belief that the information could not have been retained by the unauthorized recipient

Presumption of Breach

- Factors to Determine if Breach Reporting is Required
  - Unauthorized acquisition, use, or disclosure of PHI is ***presumed*** to be a HIPAA breach.
  - The burden is on the covered entity or business associate to demonstrate low probability of compromise.
  - This requires a multi-factor analysis.

HIPAA Breach Risk Analysis Factors

- Factors to determine if there is a low probability of compromise:
  - The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
  - The unauthorized person who used the protected health information or to whom the disclosure was made;
  - Whether the protected health information was actually acquired or viewed; and
  - The extent to which the risk to the protected health information has been mitigated.

HIPAA Breach and Ransomware

- Ransomware is an example of how these factors can be put to work.
- In 2016, HHS/OCR published a fact sheet addressing HIPAA and ransomware.
  - That fact sheet defined a ransomware incident as a breach:

> When electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

HIPAA Breach and Ransomware

- Breach notification can be avoided if an analysis under the factors demonstrates low probability that PHI has been compromised.
  - Preservation of evidence
  - Documented investigation and security incident response procedures
  - Expert input and guidance
  - Documented analysis
  - Include other relevant factors that may have been considered

HIPAA Breach Reporting

- Requirements of Breach Notification
  - Notice to Individuals
  - Media Notice
  - Substitute Notice
  - Breach report to the U.S. Department of Health and Human Services—Office for Civil Rights (HHS/OCR)

Individual Notice

- Individual notice must be mailed via first class mail or email if the individual has provided email consent.
- Deadline for mailing is 60 days after discovery.
- Notice letters have required content set out in HIPAA.
- May have to address additional state law requirements for notice letter content.
  - But what about Massachusetts?

Individual Notice

- Notice Letter Content
  - The letter must provide a brief description of what happened
  - Include the date of the breach and the date of discovery of the breach, if known.
  - Describe the types of PHI potentially impacted (i.e. SSN, DOB, treatment information, etc.)
  - Outline steps the individuals can take to protect themselves
  - Describe what is being done to investigate the breach, mitigate the harm, and protect against future breaches.
  - Provide a contact for questions (either a toll-free number, email address, website, or postal address)

Media Notice

- Media notice is required for a breach involving more than 500 residents of a State or jurisdiction.
  - Just like notice letters, the deadline for media notice is 60 days from the date of discovery of a breach.
  - The media notice must include all the elements of the notice letter.
  - There is no requirement you ensure the media notice is actually published.

Substitute Notice

- Substitute notice addresses situations where contact information is out-of-date.
  - If there are insufficient or out-of-date addresses for 10 or more individuals, there are two options for substitute notice
    - A conspicuous posting for a period of 90 days of the covered entity's or business associate's website
    - Conspicuous notice in major print or broadcast media in the geographic areas where the individuals who are likely impacted reside.
  - Substitute notice is required to include a toll-free number that remains active for 90 days.

Report to HHS/OCR

- All breaches that require notification to individuals must also be reported to HHS/OCR.
- 500 or More Individuals
  - Report must be made to HHS/OCR contemporaneously with individual notices.
  - Reported through the HHS/OCR breach reporting portal found at https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true
  - The report to HHS/OCR must be made within 60 days of discovery of the breach.

Report to HHS/OCR

- Fewer than 500 Individuals
  - Report must be made to HHS/OCR no later than 60 days after the end of the calendar year in which the breach was discovered.
  - California Department of Public Health
    - Reporting entities have 15 days to report a breach to the California Department of Public Health.
    - Not all California entities covered by HIPAA will trigger this requirement.
    - Applies to clinics, health facilities, home health agencies, or hospices licensed under specifically listed sections.
    - California Health & Safety Code §1280.15

HHS/OCR Investigations

- HHS/OCR investigates all reported breaches involving more than 500 individuals
- HHS/OCR has the authority to investigate any reported breach involving fewer than 500 individuals
- HHS/OCR can also investigate filed complaints
- HHS/OCR has authority to issues civil money penalties and refer matters for criminal prosecution
- In my experience, HHS/OCR investigations typically take 6-12 months to complete (although longer or shorter is not uncommon)

The Constant Battle - Prevention

- **Prevention**
  - Multi-factor authentication
  - External email flagging
  - Strong spam filtering
  - Endpoint monitoring – with heuristic application
  - Secure RDP ports (strong passwords, MFA, update software, etc.)
  - Patch management
  - Complex password management
  - Firewall configuration
  - Network segmentation
  - Employee training / testing

The Human Element

- Risks cannot all be mitigated with technology … the human element is always in play
- The human user of technology – **The employee** – Is **essential to protecting network resources**
- Organizations should **establish a culture of security**
  - **Safe environment** in which to communicate
  - **Effective training** programs
  - **Efficient reporting** protocols
  - Create a **human firewall**

Breach Litigation Trends

- Litigation trends in the healthcare arena
- Plaintiffs counsel continue to search for causes of action to pursue HIPAA-related data breaches
- State laws and procedure are as important
- Anticipating litigation before a data security incident occurs

Questions?