HIPAA Breach Response, Investigation and Reporting:

How to Follow the Rules to Reduce Fines and Penalties (and What the Rules Don't Say, but You Need to Know)

Presented by:

Lani M. Dornfeld, Esq., CHPC
Member
Brach Eichler L.L.C.

973-403-3136
ldornfeld@bracheichler.com

www.bracheichler.com

The HIPAA Enforcers Are Not Fooling Around

- 10/2018 – Insurer Anthem subject to undetected continuous and targeted cyber-attack = record-setting **$16M penalty** + corrective action plan (CAP), largely due to failure to conduct enterprise-wide risk analysis and insufficient procedures to review system activity

- 2/2017 – PHI of >115k people impermissibly accessed by employees and impermissibly disclosed to affiliated physician office staff; login credentials of former employee used = **$5.5M penalty** + CAP against Memorial Healthcare System

The HIPAA Enforcers Are Not Fooling Around

- 12/2018 – Colorado hospital failed to terminate former employee's access to PHI = $111,400 penalty and CAP
- 12/2018 – Hospitalist group shares PHI with business associate without business associate agreement in place = $500,000 penalty and CAP
- 11/2018 – Allergy practice shares PHI with a reporter = $125,000 penalty and CAP
- 5/2019 – Tennessee diagnostic imaging services company pays $3M penalty + CAP when one of its FTP servers allowed uncontrolled access to its patients' PHI, permitting search engines to index the PHI of patients, which remained visible on the Internet even after the server was taken offline; >300,000 patients affected

The HIPAA Enforcers Are Not Fooling Around

1/2017 – $457k penalty + CAP assessed against Presence Health based on untimely reporting of a breach of unsecured PHI

Breach incident involved lost/missing paper-based operating room schedules, which contained PHI of 836 individuals

OCR investigation revealed that ***"Presence Health failed to notify, without unreasonable delay and within 60 days of discovering the breach, each of the 836 individuals affected by the breach, prominent media outlets (as required for breaches affecting 500 or more individuals), and OCR."***

Additional Potential Liability

- State identity theft prevention laws (NJ law amended May 2019)
- State breach notification laws
- State laws requiring heightened protections of sensitive information, including, e.g., SUD patient information, mental health information, HIV/AIDS information, genetic information, etc.
- Some breach incidents result in referral to DOJ or State AGs, with additional penalties

Privacy Incident

A medical provider mails a patient's written record to the patient. The patient's name is clearly on the envelope, and the envelope is sealed. However, the address is an old address for the patient.

The recipient at the address calls the provider and states that he received the mail intended for the other individual, that he opened it and saw it was not for him and who it was from, and thereafter discarded the mail. He states he is just calling to let the provider know of the error.

Privacy Incident

Mary, an employee of a substance use disorder (SUD) treatment program, is the health care proxy/medical power of attorney for her sister. Mary's sister enters into treatment at the SUD treatment facility at which Mary works. After a few months of treatment, Mary used her own credentials (username and password) to access the EHR, and pulled up her sister's complete medical record, including psychotherapy notes from therapy sessions.

An employee reported to the privacy officer that he heard "through the grapevine" that certain employees were accessing the EHR to obtain health information about family members and others, and he had concerns this was improper.

The SUD program undertook review of EHR system access logs and was able to see Mary's activity, as well as activity of others who accessed information about ex-spouses and other employees.

Privacy Incident

A patient asks the medical office receptionist to fax certain health information to a school. The patient writes the recipient's name and fax number on a piece of scrap paper and gives it to the receptionist.

Later in the day, the receptionist remembers that she was instructed to fax the information to the school, retrieves the patient's medical record and faxes what she believes the patient asked for. The next day, the patient calls the receptionist, stating he is furious she faxed highly sensitive HIV/AIDS and SUD treatment information to his school without his authorization. The patient also files a formal complaint with the OCR.

Privacy Incident

A workforce member received an email from what looked like one of the workforce's contacts. The email content looked fairly legitimate, except in looking back on the event the workforce member noted that, in her *gut*, she felt something was off about the grammar, punctuation, and style of writing. Nonetheless, the workforce member clicked on a link in the email.

After doing so, the workforce member's computer started "acting funny," and she called the IT manager.

Upon review of the issue, the IT manager discovered that clicking on the link introduced a destructive malware software into the organization's systems.

Privacy Incident

A medical practice receptionist and medical assistant were sitting inside the reception area, with the reception "window" open to the patient waiting room. Other than the open window, the internal reception area was separated from the patient waiting area by a glass privacy wall. The medical assistant realized that a vaccination needed for the patient's appointment was not in the office. She got on the telephone to call the supplier and had a discussion about the issue. She then discussed the results of the call with the receptionist.

When she got off the phone, the patient who was the subject of this conversation walked up to the reception window and loudly complained that the office staff just breached her information because she could hear everything they were saying, including her name, during these interactions.

Privacy Incident

A medical practice receptionist took a photo on her cell phone of artwork her child made at school, that she had hanging on the corner of her computer monitor. She then posted the photograph on her social media account to show off her child's talents. Unfortunately, she did not focus on the fact that the photograph depicted not only the child's artwork but also the patient scheduler that was on her computer screen when she took the photograph.

The next day, the practice received a telephone call from someone in the community, alerting the practice to the "breach of patient information" caused by the social media post.

The patient schedule seen on the computer screen shown in the photograph included patient names, date and time of appointment, scheduled medical service, patient telephone number and other protected health information.

Breach of Unsecured PHI

- **Breach**
  - The acquisition, access, use or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule ***which compromises the security or privacy of the PHI***

- **Unsecured PHI**
  - PHI that is not rendered unusable, unreadable, or indecipherable – typically this means through encryption

Breach of Unsecured PHI

- **Breach excludes:**
  - unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate, if made in good faith and within scope of authority, and does not result in further breach
  - inadvertent disclosure by authorized person to another authorized person, without further disclosure
  - disclosure of PHI with good faith belief that unauthorized recipient would not reasonably have been able to retain the information

HIPAA Breach Notification Rule

Discovery

- Upon discovery of a breach, covered entity has 60 days to investigate and report, if required
- Date of "discovery" is first day on which the breach is known to the covered entity, or by exercising reasonable diligence would have been known to the covered entity
- Upon discovery, breach investigation must begin

Investigation: Swift Action a Must

- **Assemble a response team immediately**
  - HIPAA Privacy Officer
  - HIPAA Security Officer
  - IT Manager?
  - HR Manager?
  - Compliance Officer/Committee?
  - Need forensic IT or cyber response experts?
  - Should legal counsel be consulted? (attorney-client privilege)
  - Does leadership need to be notified?
  - Need public relations professionals?

Mitigation

- As early in the investigative process as possible, the covered entity should seek to take mitigating actions to contain the breach or prevent additional or future similar breaches

- Mitigating actions will assist in risk assessment and help reduce liability

Investigation: Careful, Planned Approach

Investigative steps flow from breadth and type of incident

- Impermissible disclosure incidents
  - ✓ Violation of minimum necessary standard
  - ✓ Mis-directed mail or fax
  - ✓ Curious staff members
  - ✓ Sharing of IT credentials
  - ✓ Allegation of over-disclosure
  - ✓ Disclosure without or beyond scope of written authorization
  - ✓ Social media disclosure
- IT incidents
  - ✓ Website breach ("contact us" or payment portal)
  - ✓ Patient portal breach
  - ✓ Phishing, malware, hacking, ransomware or similar cyber incident
  - ✓ PHI becomes publicly-facing on the internet
  - ✓ Loss/theft of computer or other electronic device
  - ✓ Unauthorized access to systems

Investigation: Who, What, When, Where, Why?

Who…

- Determine relevant individuals to interview; more interviews will likely flow from information received in initial interviews
- Ratio: 2 interviewers to 1 interviewee
- Focus questions on the Who, What, When, Where, and Why of the incident
- Conduct in private; document all interviews in writing
- Advise interviewees to maintain confidentiality of investigation
- Interview results should provide guidance to next steps

Other Investigative Steps

- Document Review and Forensic Review
  - Determine from interviews and information gathered what further documents and other information needs to be reviewed
    - ✓ Review of correspondence, audit logs, emails, social media posts, etc.
  - Determine if need IT expert for forensic review
    - Was there human input error, systems error, system flaws or weaknesses, cyber attack, other IT problem?

Risk Assessment: Guilty Until Proven Innocent

- Must conduct risk assessment: any impermissible acquisition, access, use, or disclosure of PHI is *presumed* to be a breach, unless prove otherwise through multi-factor risk assessment
- If, through risk assessment, can demonstrate there is a "low probability" PHI has been "compromised," then no mandatory reporting
  - "compromise" is not defined in the rule

Analyze Risk Assessment Factors

- ***The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification***
- ***The unauthorized person who used the PHI or to whom the disclosure was made***
- ***Whether the PHI was actually acquired or viewed (or there was only the opportunity)***
- ***The extent to which the risk to the PHI has been mitigated***
- ***Other factors as determined by the covered entity***

Breach Notification

- Notice to affected individuals must be made *without unreasonable delay*, but in no case later than sixty (60) calendar days after the date of "discovery"
  - Caveat: If law enforcement officials inform the covered entity that notice to the affected individuals will impede a criminal investigation or cause damage to national security, the covered entity must delay

Breach Notification

Additional Notices

- To the media
  - if a single breach event affects > 500 residents of the same state or jurisdiction (without unreasonable delay; but no later than 60 calendar days after discovery)
- To the Secretary of DHHS
  - if a single breach event affects ≥ 500 individuals, regardless of the state or jurisdiction (without unreasonable delay; but no later than 60 days after discovery)
  - if a single breach event affects < 500 individuals, on an annual basis (within 60 days after the end of the calendar year)
- Covered entity must maintain a breach log

Document, Document, Document…

- Investigative notes, statements, documents, reports, analyses, relevant agreements (e.g. BAAs), audit logs
  - what might OCR ask for if this issue is investigated?

- Investigative summary report
  - risk assessment

The Aftermath

Consider, document and effectuate necessary follow-up action items

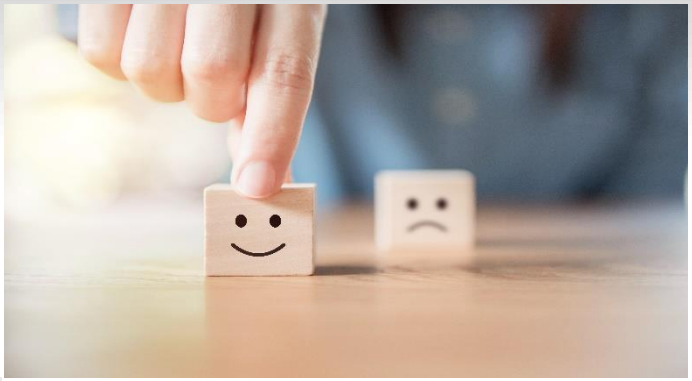
- Discipline, including potential termination
- Terminate/limit access rights
- Update policies
- Provide additional training/education
- Enhance security safeguards
- Update/execute BA agreements
- Update/perform security risk/gap analysis
- Refer to civil or criminal authorities
- Revise business associate agreements
- Update Notice of Privacy Practices
- Apologize

Responding to OCR Inquiries

- Prior to responding, gather all requested documents and information, and perform a detailed internal review
  - Identify weaknesses and consider appropriate response
  - Consider engaging legal counsel when needed
- Develop rapport and open line of communications with OCR investigator
- Demonstrate willing cooperation
- Keep track of deadlines for requests
- Consider detailed, carefully-worded written responses – cite to the law and/or DHHS guidance when possible
- Demonstrate HIPAA compliance as best as you can

Why does this matter?

Reputational Harm



Financial Loss

Civil Money Penalties

Business Interruption

DHHS “Wall of Shame”

Criminal Penalties

Lani M. Dornfeld, Esq., CHPC

Member, Health Law Practice Group
Certified in Healthcare Privacy Compliance
973-403-3136
ldornfeld@bracheichler.com
www.bracheichler.com

A Member in Brach Eichler's Health Law Practice Group, Lani Dornfeld travels between the firm's Palm Beach, FL and Roseland, NJ offices to meet client needs in both states. Lani's practice is focused on handling regulatory, corporate, and transactional matters for her clients, including hospitals, long-term care facilities, home health agencies, hospices, nursing homes, assisted living facilities, substance use disorder treatment and mental health providers, physician and dental groups, and physicians, dentists and other health care providers.

Lani has extensive experience counseling clients on regulatory and compliance matters, including HIPAA, OSHA, and corporate compliance, and assists with the development and implementation of policies, procedures, and training required by these laws. She also works with clients to investigate and manage regulatory compliance issues, including privacy and security breach situations and responses. In this regard, Lani assists clients in navigating through the complex investigation of privacy and security breach incidents, including ransomware attacks and other security breaches, and incident response and federal and state reporting obligations, as well as management of government inquiries.

Lani also represents clients in purchase and sale transactions, including due diligence, contract preparation and negotiation, and managing the closing and beyond.

Disclaimer:

This presentation and outline are designed to provide accurate and authoritative information regarding the subject matter covered. This presentation and outline should not be construed as legal advice or as pertaining to specific, factual situations. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

References

- 45 C.F.R. §§ 164.400-414
- https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
- https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html
- https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html
- https://www.hhs.gov/about/news/2018/12/11/colorado-hospital-failed-to-terminate-former-employees-access-to-electronic-protected-health-information.html
- https://www.hhs.gov/about/news/2018/12/04/florida-contractor-physicians-group-shares-protected-health-information-unknown-vendor-without.html
- https://www.hhs.gov/about/news/2018/11/26/allergy-practice-pays-125000-to-settle-doctors-disclosure-of-patient-information-to-a-reporter.html
- https://www.hhs.gov/about/news/2019/05/06/tennessee-diagnostic-medical-imaging-services-company-pays-3000000-settle-breach.html
- https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/presence/index.html