Cyber Threats, Data Breaches, Privacy Issues and the Health Care Provider– What Are the State Enforcers Looking At?

HCCA's 22nd Annual Compliance Institute
Las Vegas, NV | April 16, 2018

Presented by

George Breen
Shareholder
Epstein Becker Green
Gbreen@ebglaw.com

Esther Chavez
Senior Assistant Attorney General
Office for the Texas Attorney General
Esther.Chavez@oag.texas.gov

Agenda

1. Introduction
2. Federal Regulation and Oversight
3. State Regulation and Oversight
   i. States' Enforcement Authority
   ii. State Law Trends
4. Enforcement Trends
   i. Federal HHS OCR
   ii. States' Attorneys General
5. You've Been Hacked! Tips & Best Practices
6. Questions

Introduction: 2017 - The Year of the Cyberattacks

- 1579 data breaches in 2017
  - Medical/health sector accounted for 23.7% of all breaches.
- 5.6 million patient records compromised in 2017
- 21% increase in cyberattacks from 2016
- Cost large U.S. enterprises $1.3 million on average

Federal Oversight: HHS and the Office for Civil Rights

- HHS OCR enforces the HIPAA Privacy, Security and Breach Notification Rules.
- Violations may result in Civil Monetary Penalties, and in some cases, criminal penalties enforced by the U.S. Department of Justice may apply.
- Issues of common noncompliance may include:
  - Impermissible uses and disclosures of PHI
  - Lack of PHI safeguards
  - Patients' lack of access to their PHI
  - Use or disclosure of more than the minimum necessary PHI
  - Lack of administrative ePHI safeguards

Federal Oversight: Penalties (including inflation adjustment)

Violation Category	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$112–$55,910	$1,667,299
(B) Reasonable Cause	$1,118–$55,910	$1,667,299
(C)(i) Willful Neglect-Corrected w/in 30 days	$11,182–$55,910	$1,667,299
(C)(ii) Willful Neglect-Not Corrected w/in 30 days	At least $55,910	$1,667,299

Federal Oversight: HIPAA Rules

1. HIPAA Privacy Rule
2. HIPAA Security Rule
3. HIPAA Breach Notification Rule

Federal Oversight: HIPAA Rules

- Privacy Rule
  - Establishes national standards to protect the privacy of PHI, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.
- Security Rule
  - Specifies safeguards that Covered Entities and their Business Associates must implement to protect the confidentiality, integrity, and availability of ePHI.
- Breach Notification Rule
  - If breach impacts more than 500 people, must notify affected individuals, and in some cases, the media, without unreasonable delay **and no more than 60 days** after the **discovery** of the breach.

PHI includes information that relates to all of the following:

- The individual's past, present, or future physical or mental health or condition.
- The provision of health care to the individual.
- The past, present, or future payment for the provision of health care to the individual.
- PHI includes many common identifiers, such as name, address, birth date, and Social Security number.

Federal Oversight: CMS Guidance on Ransomware and HIPAA

OCR Guidance (July 2016)

- OCR issued guidance to help companies understand and report breaches.
- Explains that **any** encryption of ePHI by a third party as a result of a ransomware attack **results in an OCR breach.**
- OCR issued a checklist for companies to follow when responding to ransomware attacks:
  - Execute mitigation and contingency plan
  - If more than **500 people** affected → Report the incident no later than **60 days**
- OCR's "Wall of Shame"

Federal Oversight: Has a breach occurred?

- Under HIPAA, a breach is defined as "…the acquisition, access, use or disclosure of PHI in a manner not permitted under [HIPAA] which compromises the security or privacy of the PHI."
- According to HHS guidelines, the burden of proof in determining whether there was a **reportable** breach of patient data during a ransomware attack **is on the provider.**
  - Difficult when providers **can't rule out** that the hacker did not have access to patient information.
- However, in the eyes of OCR, **any encryption** of ePHI by a third party as a result of a ransomware attack is **an OCR breach if more than 500 people** have been affected.

Federal Oversight: Texting Patient Information

CMS Guidance (Dec 2017)

- Texting **patient information** among members of the health care team is permissible only if accomplished through a secure platform.
- Texting of **patient orders** is prohibited regardless of the platform utilized.
- Computer Provider Order Entry is the preferred method of order entry by a provider.
- In order to remain compliant with all Conditions of Participation and Conditions of Coverage, all providers must utilize and maintain systems that are secure, encrypted and minimize the risks to patient privacy and confidentiality.

EPSTEIN BECKER GREEN

State Regulation and State Attorney General Enforcement

States' Authority - Consumer Protection UDAP/DTPA Laws

General consumer protection UDAP/DTPA laws enacted in 50 states and the District of Columbia

- Prohibit unfair, false, misleading, or deceptive acts and practices.
- Liberally construed.
- Grant broad investigative authority to States AGs.
- Remedies:
  - Civil penalties, injunctive relief, consumer restitution and attorney's fees.

States' Authority: Data Security and Breach Notification Laws

49 States have data breach notification and/or data security laws.

- Some expressly mandate reasonable data security measures to prevent unauthorized use or disclosure.
- All require timely **notice of breach to consumers** – with certain exceptions.
- Some require **notice to the State Attorney General.**
- Some require notice to credit reporting agencies.
  - *Tex. Bus. & Com. Code § 521.053(h)*
- Some regulate the contents of a notice.
  - *N.C. Gen. Stat. Ann. § 75-65* (requiring notice of breach to be "clear and conspicuous" and in one of the methods proscribed by the statute.)
- Some require credit monitoring.
  - *Cal. Civil Code § 1798.82(d)(2)(G)* (requiring 12 months of "appropriate identity theft prevention and mitigation services.")
  - *Conn. Gen. Stat. Ann. § 36a-701b* (requiring minimum 12 months of "appropriate identity theft protection, and, if applicable "mitigation services.")

States' Authority – HIPAA

- **42 USC 1320d-5(d)):**
  - State Attorneys General can bring civil actions in federal court on behalf of state residents "threatened or adversely affected by" a violation of the HIPAA Privacy or Security Rules.
  - Available remedies and sanctions: injunctive relief; statutory damages of $100 per violation, not to exceed $25,000; and attorneys' fees and costs.
  - State Attorneys General are required to serve prior written notice on the Secretary of HHS, where feasible, in which case HHS can intervene in the action.
  - If HHS brings prior action, it preempts an identical state action to enforce HIPAA.
  - However, State Attorneys General remain able to bring actions under their own state laws that are not in conflict with HIPAA.

EPSTEIN BECKER GREEN

State Law Changes and Trends

State Law Changes and Trends

- Data security and breach laws in 12 states amended in 2017
  - Expanding universe of types of data whose improper disclosure will require notice.
    - Medical information, health insurance information, biometrics.
  - Adding strict deadlines for providing notice.
  - Requiring notice to state attorney general.
  - Being prescriptive regarding contents of consumer notice.

State Law Changes and Trends

- All 50 States now have data breach notification laws
  - Alabama – effective May 1, 2018
    - Includes requirement to maintain reasonable cybersecurity measures
  - South Dakota – effective July 1, 2018
- Notification period varies
  - Vermont – A "data collector" must notify the Attorney General within **14 days** of notice or discovery of the breach, and consumers within **45 days**
  - North Carolina – Must notify the Consumer **and** the Attorney General within **15 days** of a breach
  - Compare with HIPAA Breach Notification Rule – Must notify without unreasonable delay and no more than **60 days** after notice or discovery

State Law Changes and Trends

Trends in changes to breach notification and data security laws:

- Expanding the universe of the type of data which must be protected and which triggers notification requirement to consumers in the event of breach
  - E.g. Medical information, health insurance information, biometrics
- Adding stricter and shorter deadlines for providing notice
- Requiring notice to the state attorney general
- Prescriptive requirements regarding the contents of a notice to consumers AND regarding reasonable safeguards required to protect consumer information
- Requiring free credit reporting to affected individuals

EPSTEIN BECKER GREEN

Enforcement Trends

HHS OCR and State Attorneys General

Trending Areas of HHS OCR Enforcement

- Failure to have a good security management process.
- Failure to timely report a breach.
- Lack of encryption.
- Inadvertent disclosure.

Settlements and Civil Monetary Penalties imposed by HHS-OCR are **increasingly costly**

Trending Areas of HHS OCR Enforcement: Failure to have a satisfactory security management process

FileFax, Inc. (Feb. 2018)

- Agreed to pay $100,000 out of receivership estate to HHS-OCR to settle potential violations of the HIPAA Privacy Rule
- OCR received an anonymous complaint in February 2015 that an individual transported medical records obtained from Filefax to a shredding and recycling facility on February 6 and 9, 2015.
- OCR opened an investigation, which confirmed that an individual had left medical records of approximately 2,150 patients at the shredding and recycling facility, and that these medical records contained patients' protected health information (PHI).

Trending Areas of HHS OCR Enforcement: Failure to have a satisfactory security management process

Metro Community Provider Network (April 2017)

- Reached a $400,000 settlement for lack of security management process to safeguard ePHI.
- Hacker accessed multiple employee's email accounts in **January of 2012** and obtained ePHI of 3,200 individuals.
- OCR investigation revealed that although MCPN took the necessary corrective action to address the phishing incident, MCPN failed to conduct a risk management **until February 2012**.
- Prior to the breach, OCR contended that MCPN had failed to conduct **any** risk analysis to assess the risks and vulnerabilities in its ePHI environment, and consequentially, had not implemented any corresponding risk management plans to address the risks and vulnerabilities that would be identified in a risk analysis.
- When MCPN did conduct a risk analysis, OCR contended it was insufficient to meet the requirements of the **Security Rule.**

Trending Areas of HHS OCR Enforcement: Failure to have a satisfactory security management process

- *Fresenius Medical Care* (Feb 2018)
  - Reached a $3.5 million settlement to settle federal claims alleging lax data security practices that led to **five breaches** of electronic protected health information and exposed data of 521 patients
  - 5 breaches occurred between February and July of 2012, and are linked to some version of theft (stolen desktop computers, USB drive, hard drive, etc.)
  - As part of the settlement, Fresenius will:
    - Complete a risk analysis and risk management plan
    - Update facility access controls
    - Develop an encryption report
    - Update employees on new policies and procedures

TAKEAWAY: Number of affected individuals isn't the most important thing; repeated failure to implement policies and procedures to safeguard equipment can be costly.

Trending Areas of HHS OCR Enforcement: First Enforcement Action for failure to timely report a breach

- *Presence Health* (Jan 2018)
  - $425,000 settlement with OCR for failing to report a breach in a timely manner.
  - Discovered in October 22, 2013 that paper-based operating room schedules, which contained the PHI of about 836 individuals, was missing from one of its surgery centers.
  - Reported the breach to OCR **four months** later on January 31, 2014
    - Also did not notify affected individuals and the media within 60 day HIPAA mandated timeframe.
  - During its investigation OCR says it discovered breaches affecting fewer than 500 individuals that were also not adequately reported in a timely manner.

TAKEAWAY: Prompt investigation and assessment is critical when a possible breach of PHI is suspected. Timely reporting is key.

Trending Areas of HHS OCR Enforcement: Lack of Encryption

- *Children's Medical Center of Dallas* (Feb 2017)
  - $3.2 million CMP.
  - Hospital had two thefts:
    - Loss of unencrypted, non-password protected Blackberry in 2010
      - Contained ePHI of approximately 3,800 individuals
    - Theft of unencrypted laptop in 2013
      - Contained ePHI of 2,462 individuals
  - OCR Investigation found that hospital failed to implement risk management plans, and failed to deploy encryption or an equivalent alternative measure on all of its laptops, work stations, mobile devices and removable storage media until April of 2013.

TAKEAWAY: Failure to encrypt mobile devices, employ equivalent measures, invites trouble.

Trending Areas of HHS OCR Enforcement: Lack of Proper BAA

- *North Memorial Health Care of Minnesota* (May 2016)
  - Agreed to pay $1.55 million to OCR after it failed to identify Accreditive Health as a business associate.
  - North Memorial filed a breach report when an unencrypted, but password-protected laptop was stolen from an Accreditive member's vehicle, compromising the data of 9,497 individuals.
- *Center for Children's Digestive Health* (April 2017)
  - $31,000 settlement with OCR for not having proper business associate agreement in place.

Trending Areas of HHS OCR Enforcement: Inadvertent Disclosure

21st Century Oncology, Inc. (Dec 2017)

- Agreed to a **$2.3 million** settlement and to implement a Corrective Action Plan
- FBI notified 21CO that patient information was illegally obtained by a third party and produced 21CO patient files to an FBI informant. As part of its internal investigation, 21CO determined that attacker may have accessed 21Co's network SQL database as early as October 3, 2015, through the remote desktop protocol form an exchange server within 21CO's network. 21CO determined that **2,213,597** individuals were affected.
- OCR contended that its subsequent investigation revealed that 21CO:
  - Failed to conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI.
  - Failed to implement security measures sufficient to reduce risks and vulnerabilities to appropriate level.
  - Failed to implement procedures to regularly review records of information system activities.
  - Disclosed PHI to third party vendors **without a written BAA.**

In addition to the $2.3 million, 21CO must complete a risk analysis and management plan, develop a Corrective Action Plan, revise its policies and procedures, educate its workforce, provide all maintained BAAs to OCR, and submit an internal monitoring plan.

Trending Areas of HHS OCR Enforcement: Inadvertent Disclosure

Memorial Hermann Health System (May 2017)

- $2.4 million settlement with OCR over allegations of disclosing the name of a patient who was arrested, violating HIPAA Rules.
- Disclosed the patient's name through press releases issued to 15 media outlets and reporters between Sept. 15 and 19, 2015.
- In addition, MHHS is required to update its policies and procedures on safeguarding private information from impermissible uses and to train its workforce.

Trending Areas of HHS OCR Enforcement: Inadvertent Disclosure

- *Memorial Healthcare Services* (Feb 2017)
  - $5.5 million settlement with OCR over allegations that employees impermissibly accessed, and disclosed to affiliated physician office staff, the PHI of 115,143 individuals.
- *St. Luke's-Roosevelt Hospital Center, Inc*. (May 2017)
  - $387,200 settlement after one of its offices faxed a patient's medical record, which included information on his HIV status, sexual orientation, medical care and mental health diagnosis **to the patient's employer.**

Overview: States' Enforcement Process

- Examples
  - Equifax: MA files suit; multiple states launch investigations
  - Uber: WA and PA file suit; multiple states investigate
- States' consumer laws grant investigative authority to:
  - Seek production of documents and answers to interrogatories via civil investigative demand (CID)
  - Take oral statements

States' Multistate Enforcement

- Joint investigation by states with a common interest in a matter
- Process permits states to pool resources and expertise
- Process permits company to deal with one rather than multiple state regulators
- Serve to harmonize norms across jurisdictions

Trends in State Enforcement

- Failure to Timely Report a Breach
- Misleading and/or Inadequate Privacy Practices
- Lack of Reasonable Security Measures
- Compliance Terms Required

Trends in State Enforcement: Failure to Timely Report a Breach

- *CoPilot Provider Support Services, Inc.* (NY – June 2017)
  - Will pay $130,000 and agreed to settle with NY AG after suffering data breach compromising more than 220,000 patient records in **October of 2015**, but not to reporting the breach to patients until **January 2017.**
  - CoPilot blamed ongoing FBI investigation, but New York argued that the FBI never explicitly told the company to hold off on reporting.
    - As part of agreement, CoPilot acknowledged that it cannot postpone a breach report "unless explicitly directed in writing" by law enforcement.

Trends in State Enforcement: Misleading Claims Regarding Privacy Practices

Cardiio, Runtastic and Matis (NY – March 2017)

- All three mobile health apps had privacy policies that relied on consumer consent by default, without requiring express consent.
- NY AG criticized Cardiio for a statement in its privacy policy that allowed for the disclosure of user information if "it believed in good faith that disclosure was reasonably necessary to protect the property or rights of Cardiio, third parties or the public at large."
  - Conferred "virtually unlimited discretion" to Cardiio in disclosing user's personal information.
- Settlements required developers to r**equire affirmative consent and disclose that they collect and share information that may become personally identifiable.**
  - This includes users GPS location, unique device identifier, and "de-identified" data that third parties may be able to use to re-identify specific users.

Takeaway: Mobile health app and software developers should carefully evaluate how individual states could monitor claims and their privacy practices in addition to, or in lieu of, federal regulators.

Trends in State Enforcement: Lack of Reasonable Security Measures

Cottage Health System (CA – Dec 2017)

- In 2013, CA AG discovered two separate incidents in which *Cottage Health* made over 50,000 patients' confidential medical information publicly viewable online.
- Settlement requires:
  - **$2 million** payment.
  - Take steps to update health care information security program for the next three years.
  - Designate an employee to oversee compliance with state and federal privacy laws.
  - Complete and deliver an annual privacy risk assessment to the CA AG's office for the next two years.

Trends in State Enforcement: Lack of Reasonable Security Measures

Virtua Medical Group (NJ – April 2018)

- Agreed to a $418,000 settlement with the NJ AG after exposing over 16,00 patient's medical information
- Privacy breach occurred when Virtua's transcription vendor – Best Medical Transcriptions – updated software on a password-protected FTP website where the transcribed documents were kept.
  - During the update, the vendor unintentionally misconfigured the web server, allowing the FTP site to be accessed without a password.
- Breach unearthed when Virtua received a phone call from a patient who said her daughter had found portions of her medical records from Virtua Gynecological Oncology Specialists on Google, according to authorities.
  - Virtua was not aware of the source of the information at the time because Best Medical hadn't notified the health network of the breach.

Takeaway: Fully vet vendors for their security practices.

Trends in State Enforcement: Lack of Reasonable Security Measures

Aetna (NY – Jan 2018)

- In 2017, Aetna disclosed patients' HIV status when, through the clear window of the envelope, over 7,000 letters were sent that clearly indicated the patient was taking HIV drugs.
- NY-AG settlement requires *Aetna* to pay **$1.15 million in penalties**, change its privacy practices and hire an independent consultant to monitor and report the settlement's injunctive provisions.
- This is **in addition to a $17 million** class action pursued by private plaintiffs.

Trends in State Enforcement: Recent Multistate Settlements

47 States and D.C.

- *Target* (May 2017)
  - Settled with 47 States and D.C. for **$18.5 million** following 2013 security breach affecting more than 70 million consumers.

32 States

- *Nationwide Mutual Insurance* (Aug 2017)
  - Settled with Attorneys General of 32 states for **$5.5 million** following 2012 data breach affecting 1.27 million consumers.

Trends in State Enforcement: Compliance Terms Required

- In addition to requiring payment of significant settlements amounts in fees, costs and/or penalties, AG settlements require compliance or injunctive terms intended to prevent future violations, such as:
  - Comprehensive information security programs;
  - Retaining executive to implement programs; and
  - Appropriate encryption policies;
  - Independent third party comprehensive security assessments;
  - Reasonable measures to control access to company networks (e.g. password rotation policies); and
  - Segmentation of cardholder data environment.

EPSTEIN BECKER GREEN

You have been hacked!

Data Breach – What Now and Best Practices

- Notification
  - Notify your **internal team**, and have a process to make sure that **other notifications** take place.
  - HIPAA requires notification no more than 60 days after a breach occurs, and OCR and State enforcement efforts have been enforcing this rule.
    - However, State reporting times may be **much shorter.**
- Investigation
  - Conduct a forensic investigation – who was behind the breach? what data was compromised? how that data was compromised?
  - If possible, conduct investigation before notifying victims. However, carefully balance speed and thoroughness.
  - Be mindful of notification requirements.
- Documentation
  - The situation, including the state of any laptops or electronic devices.
  - The forensic investigation and any steps taken before, during, or after the investigation.
  - Patients notified and timeframe for notification.

EPSTEIN BECKER GREEN

Data Breach – What now and Best Practices

- Conduct a **risk assessment** and regular **audits.**
- Provide continued HIPAA education to all employees.
- Educate and re-educate employees about how to **handle suspicious e-mails.**
- Educate and re-educate employees on **theft-prevention**
- Encrypt, encrypt, encrypt.
- Have **backup** files so as to not interrupt services in the event of an attack.
- Monitor your vendors – **Hold BAA's accountable** for their IT policies and establish a process for reporting any breaches.
- Be prepared - engage counsel and experts early.

Best Practices For Managing The Internal Investigation

- Internal Investigation
  - What Happened?
  - Why did it happen?
  - Who / what was responsible?
  - Is it fixed / mitigated?
  - Have you taken steps to ensure it won't happen again?

Best Practices for Managing The Internal Investigation

- Is Disclosure / Reporting Necessary
  - Is it a Breach?
    - Not mere violation of privacy or security regulation
    - Breach is an actual unauthorized acquisition, use or disclosure of PHI that violates the privacy rule.
    - Perform an Assessment to determine if a Breach has occurred.
    - If no Breach → No disclosure required.
- Maintain documentation of analysis

Managing The Government Enforcement Action

- Which Government Agencies May Be Involved
  - HHS Office of Civil Rights
  - FTC Bureau of Consumer Protection
  - State AGs
  - CMS
  - Considerations:
    - Are you a Medicare contractor (e.g., MA, Pt D, demonstration projects)?
    - Tricare reporting requirements.
    - Medicaid reporting requirements.
    - Does your state have a health breach notification statute? If not, is it PII requiring state notification?

Managing The Government Enforcement Action

- How Investigations May Begin
  - Media Reports
  - Covered Entity Logs / OCR Audits
  - Self-Reporting
  - Complaints
- Critical Points
  - Consumers - "gold standard" monitoring
  - Vendors
  - Prior incidents become relevant
  - Relationships
  - Senior Management Commitment

Managing The Government Enforcement Action

- HHS Resolution Agreement / CAP
  - Ongoing, 3 year compliance "contract“
  - Compliance Representative
  - Internal Monitoring Plan
  - Implementation and Periodic Reports
  - Appointment of Assessor (independent third party)
  - OCR approval of policies and procedures
  - Reportable Events
  - CMPs for CAP breach

Managing The Government Enforcement Action

- FTC Consent Decree
  - Third party assessment with certification of effective security program
  - Accountable employee(s)
  - Risk identification and assessment
  - Implementation of reasonable safeguards
  - Ongoing evaluation and adjustment
- State Settlement or Judgment
- Penalties

EPSTEIN BECKER GREEN

QUESTIONS?

Presented by

George Breen
Shareholder
Epstein Becker Green
Gbreen@ebglaw.com

Esther Chavez
Senior Assistant Attorney General
Office of the Texas Attorney General
Esther.Chavez@oag.texas.gov

51