Data Protection, Privacy and Security in the Health Care Industry Year in Review; State Enforcement Focus Areas in 2018 and Outlook for 2019

HCCA's 23nd Annual Compliance Institute

Boston, MA | April 8, 2019

Presented by

George B. Breen, Esq.
Shareholder
Epstein Becker Green
Gbreen@ebglaw.com

Sara Cable, Esq.
Director of Data Privacy & Security
Office of the Massachusetts Attorney General
Sara.cable@mass.gov

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

Federal Oversight & State Authority

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

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

All 50 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.")
  - (as of April 10, 2019). *Mass. Gen. Laws c. 93H, § 3A* (requiring minimum 18 months of "credit monitoring services" if SSN breached; 42 months if entity breached is a consumer reporting agency)

Enforcement Trends
HHS OCR

2018 HHS OCR Enforcement

- In 2018, OCR settled 10 cases and secured one judgment, together totaling $28.7 million. **This total surpassed the previous record of $23.5 million from 2016 by 22 percent.**
- In addition, OCR also achieved the single largest individual HIPAA settlement in history of $16 million with Anthem, Inc., representing a nearly three-fold increase over the previous record settlement of $5.5 million in 2016.
- Trends in HHS OCR Enforcement
  - Failure to have a good security management process.
  - Lack of encryption
  - Inadvertent disclosure
  - Failure to obtain business associate agreements

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

Anthem, Inc. - 10/15/18

- Hackers gained access to Anthem's computer system when one employee at a Anthem subsidiary responded to a spear phishing email. Hacker stole ePHI of nearly 79 million people. Anthem failed to conduct risk analysis, had insufficient procedures to regularly review information system activity; failed to respond to known security incidents, and failed to implement adequate minimum access control.
- Penalty: $16 million

Pagosa Springs Medical Center (PSMC)- 12/11/18

- Failed to remove former employee's access to web-based scheduling calendar, which contained PHI of 557 patients. Also, failed to obtain BAA with calendar company (Google) and therefore, disclosed PHI to them as well.
- Penalty: $111,400

Trending Areas of HHS OCR Enforcement: Failure to encrypt

- Cottage Health – 12/12/18
  - Two breaches of unsecured electronic protected health information (ePHI) affecting over 62,500 individuals, one in December 2013 and another in December 2015. Failed to conduct an accurate and through assessment of the potential risks and vulnerabilities to the ePHI; Failed to implement security measure; Failed to implement security measures; Failed to perform periodic technical and non-technical evaluations; and Failed to obtain a written business associate agreement with a contractor that maintained ePHI on its behalf.
  - Penalty: $3 million
- The University of Texas MD Anderson Cancer Centers - 06/18/18
  - Failure to encrypt inventory of electronic devices containing ePHI
  - Penalty: $4.3 million

Trending Areas of HHS OCR Enforcement: Inadvertent disclosure

- Allergy Associates of Harford, P.C. – 11/26/18
  - Impermissibly disclosed a patient's protected health information to a reporter. Failed to take any disciplinary action against the doctor or take any corrective action following the impermissible disclosure to the media
  - Penalty: $125,000
- Boston Medical Center (BMC), Brigham and Women's Hospital (BWH), and Massachusetts General Hospital (MGH) - 09/20/18
  - Compromised patients' PHI by inviting film crews on the premises to film an ABC television network documentary series without first obtaining authorization from patients
  - Penalty: $999,000

Trending Areas of HHS OCR Enforcement: Lack of Business Associate Agreement

- Pagosa Springs Medical Center (PSMC) - 12/11/18
  - Failed to obtain BAA with calendar company (Google) and therefore, disclosed PHI to them as well.
- Advance Care Hospitalist PL (ACH) – 12/4/18
  - Failed to enter into business associate agreement with the individual providing medical billings services to ACH, as required by HIPAA.
  - Failed to adopt any policy requiring business associate agreements until April 2014.
  - Although in operation since 2005, the company had not conducted a risk analysis or implemented security measures or any other written HIPAA policies or procedures before 2014.

A Closer Look: State Enforcement

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.

Multi-State Enforcement

First Multi-State HIPAA data breach lawsuit

- On December 3, 2018, 12 state Attorneys Generals led by Attorney General filed a multi-state suit against an electronic medical records company in connection with a 2015 data breach. The data breach compromised the data of more than 3.9 million people
  - Medical Informatics Engineering, Inc. (MIE) is an Indiana medical software company that operates a communication network allowing healthcare providers to transmit and share patient related electronic communications.
  - Between May 7, 2015 and May 26, 2015, hackers infiltrated the MIE system and accessed:
    - Patient names,
    - Mailing and email addresses,
    - Dates of birth,
    - Social security numbers,
    - Lab results,
    - Dictated reports, and
    - Medical conditions on the alleged inadequately protected computer systems of MIE.

Multi-State Enforcement

Non PHI Multi-State Data Breach Suit

- Uber
  - State Attorneys General for all 50 states reach $148 million settlement with Uber to address the company's one-year delay in reporting a data breach to approximately 600,000 drivers nationwide.
- Neiman Marcus
  - State Attorneys General for 43 states reach $1.5 million settlement with the Neiman Marcus Group to resolve an investigation into a data breach the Dallas-based retailer disclosed in January 2014. The breach exposed 370,000 customer credit card data at 77 Neiman Marcus stores nationwide.
- Target
  - State Attorneys General for 47 states reach $18.5 million settlement with Target to resolve a multistate investigation into the retailer's 2013 data breach that compromised tens of millions of customers' credit and debit card information

California

- Aetna – 1/30/2019
  - $935,000 settlement resolving allegations that Aetna violated California health privacy laws in connection with its 2017 breach of patient confidentiality
  - Due to a mailing error, a vendor for Aetna sent letters to 1,991 Californians that revealed through an oversized clear window on mailed envelopes that the recipient was taking HIV-related medication.

Connecticut

- *Byrne v. Avery Center for Obstetrics & Gynecology, P.C. – 1/17/2018*
  - Connecticut Supreme Court established that there is a duty of confidentiality between a physician and patient, and patients have the right to sue should unauthorized PHI disclosure take place
  - The plaintiff, Emily Byrne, learned she was pregnant and requested that her provider not release any of her medical information to the father of the child. Byrne was no longer in a relationship with the father. Avery Center then released Byrne's information when given a subpoena.
  - The Court's decision found that the defendant did not even comply with the face of the subpoena, which required the custodian of records for the defendant to appear in person before the attorney who issued the subpoena. Instead, the defendant mailed a copy of the plaintiff's medical records directly to the court.

New Jersey

- Aetna – 10/10/2018
  - $365,211.59 settlement after the company improperly disclosed protected health information of thousands of Americans, including hundreds of New Jersey residents
  - Aetna inadvertently disclosed HIV/AIDS-related information about thousands of individuals across the U.S. – including approximately 647 New Jersey residents – through a third-party mailing on July 28, 2017. The envelopes used in the mailing had an over-sized, transparent glassine address window, which revealed not only the recipients' names and addresses, but also text that included the words "HIV Medications."
- Virtua Medical Group – 11/2/2018
  - $200,000 settlement with a now-defunct Georgia company responsible for a 2016 security lapse that allowed the public to view online patient records belonging to more than 1,650 individuals treated by doctors associated with Virtua Medical Group ("VMG")

New Jersey (cont.)

- Emblem Health – 12/11/2018
  - Fined $100,000 for a 2016 data breached that exposed the protected health information of more than 6,000 New Jersey plan members
  - EmblemHealth sent Medicare Part D Prescription Drug Plan Evidence of Coverage documents to its members with mailing labels that included beneficiary identification codes and Medicare Health Insurance Claim Numbers (HCIN), which mirror Social Security numbers

New York

- Aetna – 1/3/2018
  - $1.15 million settlement for releaving the HIV status of approximately 2,460 New York members through a mailing in July 2017 in which the envelopes' oversize transparent address window revealed text confirming the members' HIV status

- The Arc of Erie County – 8/29/2018
  - $200,000 settlement after finding that the company exposed clients' sensitive personal information on the internet for years
  - In early February 2018, The Arc of Erie County received a tip from the public that its clients' personal information was exposed on its website – including full names, social security numbers, gender, race, primary diagnosis codes, IQs, insurance information, addresses, phone numbers, dates of birth, and ages
    - A forensic investigator found that the information was publically available on the internet from July 2015 to February 2018 and affected 3,751 clients residing in New York.

Colorado

- Colorado recently passed as sweeping law to protect patient privacy (HB18-1128), which went into effect September 1, 2018.
- Colorado now requires covered entities (e.g., business entities that maintain, own, or licenses personal identifying information (PII) in the course of their business) to implement, and ensure that third-party service providers implement reasonable security procedures and practices.
- Additionally, the law requires covered entities to develop written policies and procedures concerning the destruction of paper and electronic documents that contain PII.
- Further, the law authorizes the AG to bring civil and criminal prosecution against covered entities that violate the new rules.

Legislation

California Legislation

- Recently, California State Senator Jackson and Attorney General (AG) Becerra introduced a new bill (SB561) that will expand the consumer's right to bring private lawsuits for violations of the CCPA. If passed, SB561 will:
  - (1) provide for a private right of action for all CCPA violations—not just those stemming from a data breach;
  - (2) eliminate the 30-day period for businesses to cure after receiving notice of an alleged violation; and
  - (3) allow the AG to publish guidance materials for businesses instead of allowing businesses' the option to seek specific opinions of the AG. Currently, the CCPA allows the AG office to bring action against business, in most instances, only allowing consumers to bring private action in instances of data breach resulting from a business's failure to implement reasonable security measures. If SB561 is passed, the CCPA will materially expose businesses to private actions for damages applicable to other violations under the CCPA, including failure to provide consumers with proper notifications required under the CCPA.

Washington Legislation

- On January 18, 2019, Senator Reuven Carlyle proposed the “Washington Privacy Act” (SB 5376) that would attempt to give consumers more control over the information that big tech companies and data brokers collect about them
- If enacted the bill would:
  - Require companies that collect personal data to be transparent with users about the type of information they’re recording, how they use it, and whether it is shared with third parties
  - If those companies create profiles about their users for ad targeting, they will have to disclose that before personal data is collected “including meaningful information about the logic involved and the significance and envisaged consequences of the profiling.”
  - Set new regulations for facial recognition technology, requiring companies that make the software to get consent from consumers before using it on them.
- Companies that fail to comply with the new rules could face penalties of up to $2,500-$7,500 per violation, enforced by the state attorney general.

A Closer Look: Massachusetts

Massachusetts Data Security Law

- The Massachusetts Data Security Law is considered one of the strongest in the nation. It is enforced exclusively by the Mass. Attorney General's Office.
  - It, like HIPAA, requires entities to conduct risk assessments and to develop, implement, and maintain a written information security program containing minimum administrative, technical, and physical safeguards to protect personal information held by the entity.
  - Examples of some of the required safeguards:
    - Identify and assess reasonably foreseeable risks to the security, confidentiality, and/or integrity of records containing PI;
    - Ongoing employee training and "need to know" restrictions on access to PI;
    - Oversight of the security practices of vendors who handle PI;
    - Regular monitoring, reviews, and updates to policies;
    - Specific computer system requirements, e.g. access control and secure user authentication protocols, encryption, password requirements, firewalls, security patches, malware protection, etc.

Massachusetts Data Breach Notice Law

- The Massachusetts Data Breach Notice Law (Mass. Gen. Laws c. 93H) and Data Security Regulations (201 CMR 17.00) apply to HIPAA covered entities that have PI of Mass residents, regardless of where the entity is located.
  - Generally speaking, data breach notices sent to consumers pursuant to HIPAA are "deemed compliant" with the Massachusetts data breach notice law, provided the Mass. AG office is also notified. *See* G.L. c. 93H, section 5.
  - Effective April 10, 2019, new amendments to Data Breach Notice Law will go into effect. They do not change the core requirements of the law, but will require additional information to be reported and mandatory credit monitoring services where SSNs breached.

Recent Massachusetts Settlements

Health care entities are not immune from data security problems

- **Commonwealth v. SouthShore Hospital (2012).** Hospital used vendor to transport backup tapes offsite for destruction. Tapes contained PI and ePHI of 800,000 residents but were not encrypted, and the hospital did not have a business associate agreement with the vendor. The tapes were lost en route. Parties settled for $750,000 penalty and enhanced compliance obligations.
- **Commonwealth v. Women & Infants Hospital of RI (2014).** 19 unencrypted back-up computer tapes lost during shipping, containing PI and PHI of 12,000 MA residents. Notice of the breach was also delayed. Settled case with $150,000 penalty and compliance obligations.
- **Commonwealth v. Boston Children's Hospital (2014).** BCH practitioner stored ePHI of 2,100 residents on unencrypted laptop. Laptop was stolen during travel. Case settled by $40,000 and compliance obligations.

Recent Massachusetts in HealthCare

Health care entities are not immune from data security problems

- **Commonwealth v. Beth Israel Deaconess Medical Center (2014).** BIDMC doctor used an unencrypted laptop on which the PHI of 4,000 residents and PI of 230 residents was stored. Laptop was stolen. Settled case with $100,000 penalty and compliance obligations.
- **Commonwealth v. McClean Hospital Corp. (2018).** Hospital lost four unencrypted backup computer tapes containing personal and health information of 1,500 patients, employees and deceased donors to a Brain Tissue Resource Center. Case settled with $75,000 penalty and compliance obligations.
- **Commonwealth v. UMass Memorial Medical Group Inc. and UMass Memorial Medical Center Inc. (2018).** Each entity suffered a breach that resulted when an employee was permitted to have access to PH and ePHI of a total of 15,000 patients even after entities were on notice employee was suspected of identity theft. Entities paid a total of $230,000 to resolve case.

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.

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?


Questions

Data Protection, Privacy and Security in the Health Care Industry Year in Review; State Enforcement Focus Areas in 2018 and Outlook for 2019

HCCA's 23nd Annual Compliance Institute

Boston, MA | April 7 – 10, 2019