HIPAA AND THE HITECH ACT: RECENT CASE LAW, STATUTORY CHANGES, AND PENALTY ASSESSMENTS

Rachel V. Rose, JD, MBA
1st Healthcare Compliance HIPAA Summit
November 14, 2019

Disclaimer

- **THE INFORMATION PRESENTED IS NOT MEANT TO CONSTITUTE LEGAL ADVICE. CONSULT YOUR ATTORNEY FOR ADVICE ON A SPECIFIC SITUATION.**

Overview

(1) HIPAA and the HITECH Act – an explanation and the persons covered

(2) Case Law

(3) HHS Health App FAQs

(4) Recent Statutory (Penalty) Updates and Enforcement Actions

(5) Take-Aways

HIPAA-HITECH KEY ITEMS

Who Is Under the Legal Umbrella?

- HIPAA
  - **Covered Entities -** Health Care Providers, Health Plans and Health Care Clearinghouses
  - **Business Associates** – contract w/ Covered Entities
  - **Subcontractors** – contract w/ Business Associates
- TX House Bill 300 (TX HIPAA)
  - Different definition of "covered entity" that encompasses anyone who creates, receives, maintains and transmits PHI.
- Federal Trade Commission
  - Fills the "gap" of the Federal HIPAA definitions. anyone who creates, receives, maintains and transmits PHI.

Legislative History

- 1996 -HIPAA (Public Law 104-191) – need for consistent framework for transactions and other administrative items.
- 2002 – The Privacy Rule (Aug. 14, 2002)
- 2003 – The Security Rule (Feb. 20, 2003)
- 2009 - Health Information Technology for Economic and Clinical Health ("HITECH") Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (Feb. 17, 2009)
- 2009 – The Breach Notification Rule (Aug. 24, 2009)
- 2010 – Privacy and Security Proposed Regulations (Feb. 17, 2010)
- 2013 – Omnibus Rule (Effective March 26, 2013, Compliance Sept. 23, 2013).

The Federal Trade Commission

- FTC's Health Breach Notification Rule "-requires certain businesses not covered by HIPAA to notify their customers and others if there's a breach of unsecured, individually identifiable electronic health information."
- FTC enforcement began on February 22, 2010.

According to an HHS Fact Sheet:

"The Security Management Process standard of the Security Rule includes requirements for all covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ***all*** of the ePHI the entities create, receive, maintain, or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level."

CASE LAW

Types of Violations.

- Individual disclosure.
  - Example: University of Rochester Medical Center nurse practitioner
    - Gave a list of 3,403 patient names, addresses and diagnoses to a future employer **without obtaining permission from the patients.**
- Hospital employee or contractor looks at medical records when not part of the care team and not authorized to do so.
  - Examples: VUMC, University of California Irvine Med. Ctr.
- External Security Breach.
  - Ransomware Examples: Medstar, Hollywood Presbyterian Medical Center
  - Failing to Update Patches: CHS **(notable because there is a reporting requirement under HIPAA and under SEC regs).**

Major Breaches

- Adobe (38 million customer accounts),
- Target (40 million customers),
- Snapchat (4.6 million users),
- U.S. banks (websites offline),
- HIPAA Violations (CHS, Anthem Bluecross/Blueshield, Tenet ($32.6 million) and
- Securities exchanges (infrastructure attacks).

Warner Chilcott & Physician HIPAA Violations Brought Under the False Claims Act

- "Pharmaceutical company Warner Chilcott was sentenced today in U.S. District Court in Boston to pay $125 million to resolve criminal and civil liability arising from the illegal promotion of various drugs." https://www.justice.gov/usao-ma/pr/warner-chilcott-sentenced-pay-125-million-health-care-fraud-scheme
- Warner Chilcott cooperated with the government's investigation into culpable individuals, which has led to several individual prosecutions. Among them are:
  - Former district manager Jeffrey Podolsky pleaded guilty to health care fraud in connection with manipulating prior authorizations;
  - Former district manager Timothy Garcia pleaded guilty to health care fraud in connection with manipulating prior authorizations; and
  - Former district manager Landon Eckles pleaded guilty to wrongful disclosure of individual identifiable health information, a criminal violation of the HIPAA law.

Warner Chilcott Part 2

- Rita Luthra, a Springfield, MA-based gynecologist, **was sentenced** Sept. 19 to one-year probation for a criminal HIPAA violation and obstruction of a criminal healthcare investigation.
- In April, **a jury convicted her** of allowing a pharmaceutical sales representative to access patient records and lying to federal investigators. In May, US District Judge Mark G. Mastroianni **denied a motion by Luthra's attorney** to reverse the conviction.
- In the original compliant, the Department of Justice (DoJ) alleged that Luthra allowed a Warner Chilcott sales representative to access her patients' PHI and then provided false information to HHS agents about her dealings with the drug company.

https://healthitsecurity.com/news/ma-physician-gets-1-year-probation-for-criminal-hipaa-violation

United States of America ex rel. Bashar Sean Awad, et al. v. Coffey Health System(D. Kan. 2019)

- the United States intervened for the purpose of settlement in relators' case against Coffey Health System ("CHS") for violations of submitting false claims and attestations to Medicare and Medicaid Programs pursuant to the EHR Incentive Program and received incentive payments of approximately $3 million for the reporting periods 2012 and 2013.
- according to U.S. Attorney Stephen McAllister, "Medicare and Medicaid beneficiaries expect that providers ensure the accuracy and security of their electronic health records."

COFFEY Continued

- Among other things, in order to obtain Medicare incentive payments, providers are required to specifically attest to:
  - (i) the completion of an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the electronic protected health information [created, received, maintained or transmitted] by the covered entity or business associate" (*see* 45 C.F.R. §164.308(a)); and
  - (ii) the submission of clinical quality measures ("CQM") data through CEHRT for Stage 2 meaningful use.

ATTESTATION DISCLAIMER

- **“I certify that the foregoing information is true, accurate, and complete. I understand that the Medicare EHR Incentive Program payment I requested will be paid from Federal funds, that by filing this attestation I am submitting a claim for Federal funds, and that the use of any false claims, statements, or documents, or the concealment of a material fact used to obtain a Medicare EHR Incentive Program payment, may be prosecuted under applicable Federal or State criminal laws and may also be subject to civil penalties.”**

United States of America and the State of Illinois ex rel. Amy O'Donnell v. America at Home Healthcare and Nursing Services, Ltd., Case No. 14-cv-1098 (N.D. Ill. 2018).

- Judge Robert John Blakely ruled that an FCA claim premised on a HIPAA violation met the requisite FRCP 9(b) pleading standard and should not be dismissed.
- Judge Blakely upheld the relator's claim that "HIPAA violations under 42 U.S.C. § 1302d-6(a), which criminalizes knowingly using, obtaining, or disclosing an individual's identifiable health information without authorization" were substantiated by the facts that two individuals employed by the defendants "searched confidential medical charts at different facilities to collect the names of patients they could solicit for home health services (including unnecessary services)." *America at Home*, at p. 14.
- the defendants knowingly billed the government for medical services after obtaining patients' information unlawfully; and the defendants deliberately submitted claims and cost reports to the State of Illinois and the federal government that impliedly certified compliance with Medicare laws and regulations, but knowingly failed to disclose their HIPAA violations. *Id*.

America at Home Healthcare and Nursing Services, Ltd. & Escobar

- The Court deemed this conduct to be material as defined in *Escobar.*
- [a]s in *Escobar*, Relator explicitly alleges that complying with HIPAA's criminal provisions is a condition of payment. [...] Relator also alleges that unlawfully soliciting patients through HIPAA violations goes 'to the very essence of the bargain' between the government and health care providers, because that solicitation subjects patients to abusive marketing practices and unnecessary care from providers that they trust to help them. *Id.* at p. 16.

America at Home – Getting to Damages

- the Court analogized HIPAA violations under § 1320d-6(a) to violations of the AKS. "If 'information that a hospital has purchased patients by paying kickbacks has a good probability' of affecting a payment decision, [*United States v. Rogan*, 517 F.3d 449, 452 (7th Cir. 2008)], then information that a home health agency has pilfered protected health data to solicit patients has a good probability of affecting payment decision, too." *Id*.

Negligence-based

- WV Cases
  - ***R.K. vs. St. Mary's Medical Center, Inc.* 2012 WL 5834577**
    - Hospital employee illegally accessed the plaintiff's medical records, which included psychiatric records and sent them to the plaintiff's estranged wife and her divorce attorney.
    - **WV Supreme Court held that "State common law claims for the wrongful disclosure of medical or personal health information are not inconsistent with HIPAA. Rather, …such state law claims complement HIPAA by enhancing the penalties for its violation and thereby encouraging HIPAA compliance."**
  - ***State ex rel. State Farm Mut. Aut. Insurance Co. v. Marx.*, 2012 WL 5834584**
    - *Medical records, which are the subject of discovery, can be controlled by the trial courts. Hence, State Farm did not have a "carte blanche" right to share information with National Databases.*

Negligence-based

- CT Case
  - ***Byrne v. Avery Center for Obstetrics and Gynecology* SC 18904 (Nov. 11, 2014).**
  - A patient advised her physician not to provide information to her significant other. The significant other filed a paternity suit and issued a subpeona to the physician's office. The health center, instead of alerting the patient or fighting the subpeona, simply gave the records over.
  - The CT Supreme Court held that HIPAA does not preempt against negligence claims for a breach of privacy. Regulations of HHS implementing HIPAA may inform the applicable standard of care in certain circumstances.

Negligence-based (cont.)

- NC Case
  - ***Acosta v. Byrum*, 638 S.E.2d 246 (N.C. Ct. App. 2006)**
    - The patient was treated by Dr. Faber, who gave his access code to a third party, who, in turn, viewed his records.
    - Take aways: (1) not a malpractice claim, so no expert certification; (2) while HIPAA does not provide a private right of action, the it may be used to establish an appropriate standard of care in a negligence claim.
- 2014 Tenet settlement – class action filed in 1997, which settled for $32.5 million for records left in a parking lot in April 1996.

Statutory

- Texas Health and Safety Code §241.152(a), which applies to hospitals, their employees and agents - prohibits the disclosure of "healthcare information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative."
- Texas Health and Safety Code §241.155 - requires that hospitals adopt safeguards for the PHI that it maintains.
- **If a person is aggrieved due to the "unauthorized release of confidential healthcare information," then pursuant to the Texas Health and Safety Code §241.156(a), an action may be brought for both injunctive relief, as well as damages.**

AREAS OF UPDATE

Penalties, Health App FAQs and HITECH Act

Penalties

- In the April 30, 2019 *Federal Register* (84 Fed. Reg. 18151), HHS issued its "Notification of Enforcement Discretion Regarding HIPAA Civil Monetary Penalties".
- Section 13410(d) of the HITECH Act created four categories of HIPAA violations with corresponding penalty tiers:
  - Tier 1 – the person did not know (and, by exercising reasonable diligence, would not have known) that the person violated the provision;
  - Tier 2 – the violation was due to reasonable cause, and not willful neglect;
  - Tier 3 – the violation was due to willful neglect that is timely corrected; and
  - Tier 4 – the violation was due to willful neglect that is not timely corrected.

New Penalties

Culpability	Minimum Penalty/Violation	Maximum Penalty Violation	2009 Annual Limit	2019 Annual Limit
Tier 1	$100	$50,000	$1,500,000	$25,000
Tier 2	$1,000	$50,000	$1,500,000	$100,000
Tier 3	$10,000	$50,000	$1,500,000	$250,000
Tier 4	$50,000	$50,000	$1,500,000	$1,500,000

HHS Health App FAQs

- Does HIPAA Require a CE or its EHR System developer to enter into a BAA w/ an app designated by the individual in order to transmit ePHI to the app?
- **Short Answer:** It depends.
- **Long Answer:"** HIPAA does not require a covered entity or its business associate (e.g., EHR system developer) to enter into a business associate agreement with an app developer that does not create, receive, maintain, or transmit ePHI on behalf of or for the benefit of the covered entity (whether directly or through another business associate).
- However if the app was developed to create, receive, maintain, or transmit ePHI on behalf of the covered entity, or was provided by or on behalf of the covered entity (directly or through its EHR system developer, acting as the covered entity's business associate), then a business associate agreement would be required."

FAQs Part II

- **Question: What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?**
- **Answer: "Under the individual right of access, an individual may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii).** For instance, an individual may request that their unencrypted ePHI be transmitted to an app as a matter of convenience. In such a circumstance, the covered entity would not be responsible for unauthorized access to the individual's ePHI while in transmission to the app. With respect to such apps, the covered entity may want to consider informing the individual of the potential risks involved the first time that the individual makes the request."

FAQs - Liability

- **The answer depends on the relationship between the covered entity and the app. Once health information is received from a covered entity, at the individual's direction, by an app that is neither a covered entity nor a business associate under HIPAA, the information is no longer subject to the protections of the HIPAA Rules.** If the individual's app – chosen by an individual to receive the individual's requested ePHI – was not provided by or on behalf of the covered entity (and, thus, does not create, receive, transmit, or maintain ePHI on its behalf), the covered entity would not be liable under the HIPAA Rules for any subsequent use or disclosure of the requested ePHI received by the app. For example, the covered entity would have no HIPAA responsibilities or liability if such an app that the individual designated to receive their ePHI later experiences a breach.
- **If, on the other hand, the app was developed for, or provided by or on behalf of the covered entity – and, thus, creates, receives, maintains, or transmits ePHI on behalf of the covered entity – the covered entity could be liable under the HIPAA Rules for a subsequent impermissible disclosure because of the business associate relationship between the covered entity and the app developer**. For example, if the individual selects an app that the covered health care provider uses to provide services to individuals involving ePHI, the health care provider may be subject to liability under the HIPAA Rules if the app impermissibly discloses the ePHI received.

Areas of Update

- Section 13410(c)(3), HITECH Act, Pub. L. 111-5 (Feb. 2009) requires HHS to established a methodology to provide a percentage of the civil monetary penalties ("CMPs") collected to individuals who are harmed by HIPAA/HITECH Act violations. Although this was supposed to be accomplished three years after the enactment of the HITECH Act, recently, an advance notice of proposed rulemaking ("ANPRM") was published by the Office of Information and Regulatory Affairs, Office of Management and Budget, Executive Office of the President. *See*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

Areas of Update Part II

- HHS Report – *Health Information Privacy Beyond HIPAA: A 2018 Environmental Scan of Major Trends and Challenges*
- 42 CFR Part is a federal law designed to protect individuals' confidentiality when seeking treatment for substance disorders from federally assisted programs. In 2018, the Substance Abuse and Mental Health Services Administration ("SAMHSA"), building on the March 21, 2017 final rule that modernized the Confidentiality of Alcohol and Drug Abuse Patient Records (now the Confidentiality of Substance Use Disorder Patient Records) and the supplemental notice of proposed rulemaking ("SNPRM"), issued a final rule. SAMHSA, https://www.samhsa.gov/health-information-technology/laws-regulations-guidelines (last visited June 3, 2018).
- *See*, https://www.regulations.gov/document?D=HHS-OS-2016-0005-0377 (Feb. 17, 2017).
- RIN: 0930-AA21, https://www.regulations.gov/document?D=HHS-OS-2016-0005-0378 (last visited June 3, 2018).
- 83 Fed. Reg. 239 (Jan. 3, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-01-03/pdf/2017-284

ENFORCEMENT ACTIONS

University Of Rochester Medical Center Fined $3 Million

- “One of New York state’s largest health systems, must pay $3 million for failing to encrypt mobile devices such as laptops and flash drives that contained patient data, HHS.”

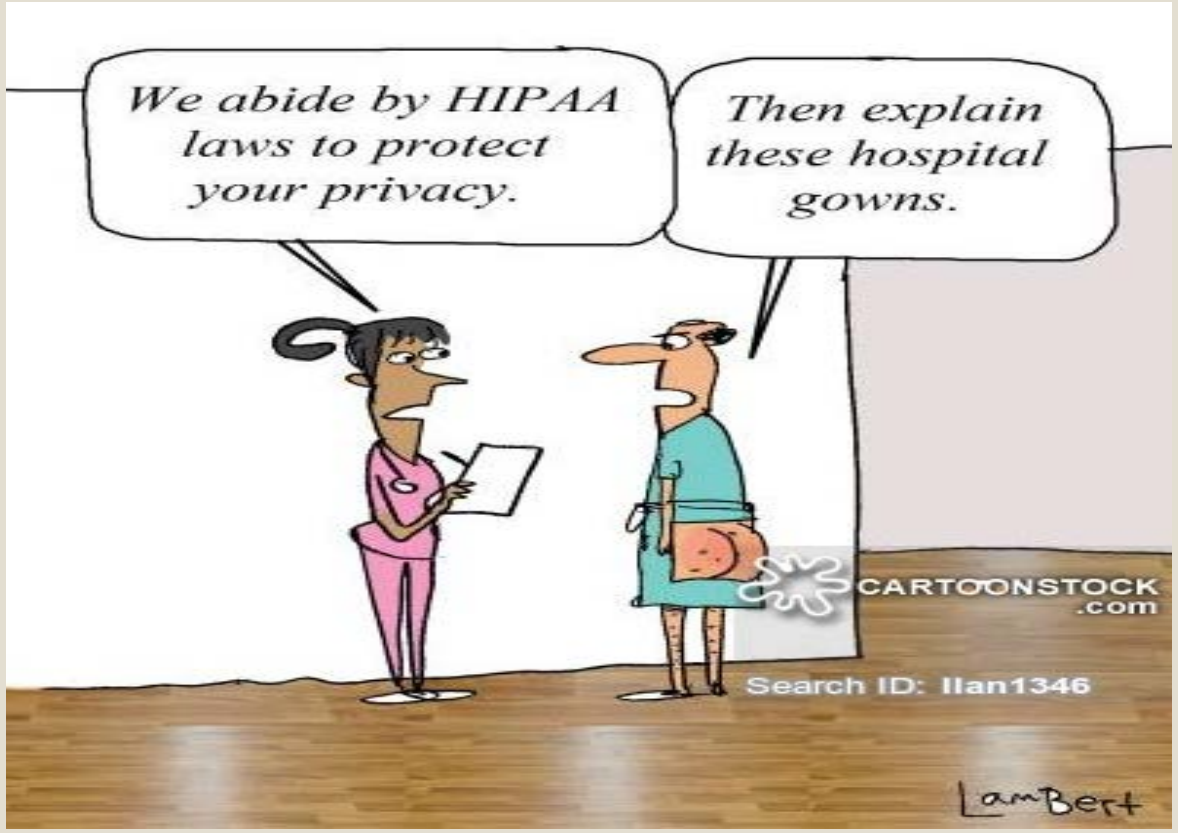
- “Found that the medical center **didn’t conduct a company-wide risk analysis, apply security measures that would reduce these risks and vulnerabilities, or implement a system that encrypts and decrypts electronic health information**.”

Florida health system pays $2.1 million HIPAA fine

- U.S. Department of Health and Human Services has imposed a civil money penalty of $2,154,000 against Jackson Health System (JHS) for violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Breach Notification Rules between 2013 and 2016.
- On August 22, 2013, JHS submitted a breach report to OCR stating that its Health Information Management Department had lost paper records containing the protected health information (PHI) of 756 patients in January 2013. JHS's internal investigation determined that an additional three boxes of patient records were also lost in December 2012; however, JHS did not report the additional loss or the increased number of individuals affected to 1,436, until June 7, 2016.
- OCR's investigation revealed that JHS failed to provide timely and accurate breach notification to the Secretary of HHS, conduct enterprise-wide risk analyses, manage identified risks to a reasonable and appropriate level, regularly review information system activity records, and restrict authorization of its workforce members' access to patient ePHI to the minimum necessary to accomplish their job duties.

TAKE-AWAYS

The Privacy Rule is Different than the Security Rule.



Take-Aways

- Any person creating, receiving, maintaining or transmitting PHI needs to protect the confidentiality, availability and integrity of the data.
- Reduced penalties do not equate to reduced compliance.
- Health Apps – it depends!
- Making false statements about HIPAA/HITECH Act Compliance can land a person in the hot seat and lead to significant financial, legal and reputational costs.
- Risk mitigation begins at the highest levels of a corporation through the corporate culture. From there, training, policies and procedures and TAP are critical.

Thank you and Questions.

Rachel V. Rose – Attorney at Law, PLLC

Houston, Texas

www.rvrose.com