THE INTERSECTION OF PRIVACY LAWS AND BIOMETRICS

Rachel V. Rose, JD, MBA

1st Healthcare Compliance Virtual Symposium

April 23, 2020

Disclaimer

The information in this program is not meant to constitute legal advice. If you need advice on a particular situation, please consult a lawyer.

AS LAWS SUCH AS THE ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT ("BIPA"), AS WELL AS SIMILAR LAWS IN TEXAS AND WASHINGTON EMERGE TO THE FOREFRONT OF LITIGATION AND ENFORCEMENT ACTIONS, LAWYERS ON BOTH SIDES OF THE AISLE, AS WELL AS COMPLIANCE OFFICERS NEED TO APPRECIATE THE LEGAL, FINANCIAL AND REPUTATIONAL RISKS. THE FOCUS ON BIOMETRICS, RECENT CASE LAW

AND THE INTERSECTION OF LAWS SUCH AS BIPA WITH HIPAA.

Introduction

Overview

- What are biometrics?
  - Laws involving biometrics and recent case law
  - The intersection of biometrics and HIPAA
    - Cultivating a culture of compliance and practical insights about what constitutes an adequate risk analysis, as well as how to address GAP items
    - Take-aways

BIOMETRICS

Webster's Dictionary Definition

1. Biometry (the statistical analysis of biological observations and phenomena).
2. The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity. (https://www.merriam-webster.com/dictionary/biometrics)

NIST and Biometrics

- The National Institute for Standards and Technology (NIST)
  - Current Special Publications
  - Superseded
- Federal Information Processing Standards (FIPS)
- Several Definitions
  - NIST SP 800-12, Rev. 1 (FIPS 201) – "A measurable physical characteristic or personal behavioral trait used to recognize the identify, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are examples of biometrics."
  - NIST SP 800-63-3 – "Automated recognition of individuals based on their biological and behavioral characteristics." (https://csrc.nist.gov/glossary/term/Biometrics)

Simply Stated Definition

"Simply put, biometric data consists of the identifying characteristics of a person's body or mind and is separated into two categories: physiological and behavioral. **Physiological biometrics** pertain to the body and include DNA, retinal scans, fingerprints or other characteristics such as the shape of a person's hand or face or the sound of their voice. **Behavioral biometrics** encompass a person's specific movements and actions or even thought patterns."

https://www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know

2 CFR § 200.82 - Protected Personally Identifiable Information ("PII")

Protected PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, **biometrics**, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts.

HIPAA & THE HITECH ACT

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.

HIPAA and the HITECH Act

- 45 CFR §§ 164.400-414 and 13407 of the HITECH Act.
- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
- Requires covered entities to notify affected individuals, U.S. Department of Health & Human Services (HHS), and in some cases, the media of a breach of unsecured PHI.
- Most notifications must be provided without unreasonable delay and no later than 60 days following the discovery of a breach.
- Notifications of smaller breaches affecting fewer than 500 individuals may be submitted to HHS annually.
- The Breach Notification Rule also requires business associates of covered entities to notify the covered entity of breaches at or by the business associate.
- **NOTE: there are three exceptions to a breach.**

Exceptions

- HIPAA allows certain disclosures without the patient's written authorization, including disclosures to other providers or third-party payers for purposes of treatment, payment, or healthcare operations; to family members or others involved in the patient's care or payment if certain conditions are met; or for certain government or public safety concerns if regulatory requirements are satisfied. (45 CFR 164.502, 164.506, 164.510 and 164.512).
- Other disclosures generally require the patient's consent or written authorization. (45 CFR 164.502).

HIPAA Marketing & Sale of PHI Provisions

- 45 CFR §§ 164.501, 164.508(a)(3)
- " The Privacy Rule defines "marketing" as making "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service." Generally, if the communication is "marketing," then the communication can occur only if the covered entity first obtains an individual's "authorization." This definition of marketing has certain exceptions." (https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/marketing/index.html)
- 45 CFR 164.502
- ***Sale of protected health information:***
- **(A)** Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.
- **(B)** For purposes of this paragraph, sale of protected health information means:
- ***(1)*** Except as provided in paragraph (a)(5)(ii)(B)(*2*) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

PII and PHI

- Privacy Rule sections CFR §§ 164.514(b), (c) apply in relation to the de-identification of PHI.
- The HIPAA Privacy Rule sets forth two acceptable de-identification methods: expert determination (an expert is utilized to ascertain that an individual could not be identified); and safe harbor (no actual knowledge that PII, **including biometrics**, can identify an individual).
- Satisfying either method would demonstrate that §164.514(a) has been met and that the likelihood of exposure is slim. Persons should also be familiar with certain exceptions, such as HIPAA's law enforcement exception (45 CFR §164.512) and the protections afforded to whistleblowers and workforce member crime victims (45 CFR §164.502(j)).
- https://www.physicianspractice.com/hipaa/intersection-hipaa-and-illinois-biometric-information-privacy-act

The Security Rule Also Applies.

It is also important to realize that because a biometric is considered to fall under the category of PHI, entities must adhere to the Security Rule in order to make sure that adequate technical, administrative, and physical safeguards are in place to protect the confidentiality, integrity, and availability of the data.

STATE BIOMETRIC PRIVACY LAWS

Texas

- Enacted in 2009
- Texas Business and Commerce Code, Title 11, Subtitle A, Chapter 503
- Prohibits the capture of an individual's biometric identifiers for a commercial purpose unless the individual is first informed and consents.
- Texas also limits the sale or disclosure of an individual's biometric identifiers except under limited circumstances.
- §503.001 – Capture or use of biometric identifier. (a) in this section**, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."**
- https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

Texas (Cont).

- **Section 503.001(b), (c)**
- (b) A person may not capture a biometric identifier of an individual for a commercial purpose **unless the person**:
- (1**) informs the individual before capturing the biometric identifier; and**
- **(2) receives the individual's consent to capture the biometric identifier**.
- (c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:
- (1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:
- (A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;
- (B) the disclosure completes a financial transaction that the individual requested or authorized;
- (C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or
- (D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;
- (2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and
- (3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

Illinois

- The Illinois Biometric Information Privacy Act ("BIPA")
- Passed in 2008
- The first state law in the country to regulate the biometric data usage.
- One key distinction between BIPA and HIPAA is that BIPA allows for a private cause of action to be brought by individuals, without showing that actual harm occurred in order to recover damages. *See* the Illinois Supreme Court's decision, *Rosenbach v. Six Flags Entertainment Corporation, et al.*, 2019 IL 123186 (Ill. 2019)
- There is no private cause of action expressly stated in HIPAA; rather, individuals typically sue under a common law negligence theory and use HIPAA as the standard to satisfy the elements of duty and breach. Causation and damages are items that still need to be proven in order to recover under a negligence case.

BIPA and HIPAA – the Intersection

- BIPA also requires adequate technical, administrative and physical safeguards. And, it applies to a variety of industries, which range from healthcare to retail to hospitality to any employer who uses fingerprint technology for time keeping purposes.
- Like PHI in relation to HIPAA, **BIPA, in most instances, requires providing notice that the biometric information is being collected and stored; providing written notice of the specific purpose and length of time for which that biometric information will be used and stored; and obtaining written consent.**
- Healthcare is a bit different than simply using a biometric to log-in to record hours worked, because the 6-7-year period of record retention serves another purpose—the continuity of patient care and treatment.

Washington

- Enacted 2017
- Chapter 19.375 RCW
- Prohibits any company or individual from entering biometric data into a database without providing notice, gaining consent and providing a mechanism for preventing the subsequent use of the biometric data for a commercial purpose. (RCW 19.375.020).
- RCW 19.375.010 - (1) "Biometric identifier" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual.
- **"Biometric identifier" does not include a physical or digital photograph, video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996.**

Washington (Cont.)

- (4) "Commercial purpose" means a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods or services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier. **"Commercial purpose" does not include a security or law enforcement purpose.**
- **RCW 19.375.040 – Exclusions**
- **(1) Nothing in this chapter applies in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley act of 1999 and the rules promulgated thereunder.**
- **(2) Nothing in this chapter applies to activities subject to Title V of the federal health insurance privacy and portability act of 1996 and the rules promulgated thereunder.**
- **(3) Nothing in this chapter expands or limits the authority of a law enforcement officer acting within the scope of his or her authority including, but not limited to, the authority of a state law enforcement officer in executing lawful searches and seizures.**

RECENT CASE LAW

Cases

- Typically Class Actions (***Jumio*** paid $7 million for BIPA violations, case filed in 2018)
  - ***Facebook***
    - Case filed in 2015
    - Alleged that Facebook collected facial recognition data on images of users in the state without disclosure, in contravention of the state's 2008 Biometric Information Privacy Act (BIPA)
    - Facebook appealed to the 7th Circuit Court of Appeals
    - **The Circuit Court concluded that "the development of face template using facial-recognition technology without consent (as alleged here) invades an individual's private affairs and concrete interests. Similar conduct is actionable at common law."**
    - United States Supreme Court denied cert.
    - **Settled for $550 million**

LOW-HANGING FRUIT & PREVENTING VIOLATIONS

The Fruit Basket

- "Health care providers and insurers are still making tons of rookie mistakes on patient privacy [and security], turning themselves into easy enforcement targets."
- Roger Severino's Comments in a February 3, 2020 Law360 Article:
  - **"For enforcement purposes, there's still a lot of low-hanging fruit."**
  - **"There are a lot of entities that are not doing the basic steps to make sure they have proper, for example, cybersecurity protections. They're not doing the comprehensive risk analyses on the front end."**
  - **"They're not implementing the proper controls on access [to patient records].**
    - **They're not having proper password policies; they're not doing system activity reviews to [make] sure that the logs that they have already in place to detect intrusion or attacks are monitored. There is also not sufficient training for privacy."**

Flouting of a Statutory Duty

- ”A wide variety of areas where entities have had breaches and have not report to us the breaches.”
- “If HIPAA enforcers unearth hidden breaches, then covered entities ‘may be accused of sweeping it under the rug,” and should “expect more vigorous enforcement.”
- **PHI “needs to be protected, which means entities have to do, first and foremost, proper risk analysis at the front end… so that they don’t have to face some very difficult questions in enforcement actions from OCR at the back end.”**

Unsecured Protected Health Information:

"PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of the HITECH Act."

Unsecured PHI

- Unsecured PHI – new term created in the HITECH Act. "PHI that is vulnerable while using technologies or methodologies that render PHI unusable, unreadable or indecipherable to unauthorized individuals."
- Examples:
  - **Good faith, unintentional acquisition, access or use of PHI:** A billing employee receives and opens an email containing PHI about a patient, which was mistakenly sent. The billing employee notices that he/she is not the intended recipient, alerts the nurse of the misdirected email then deletes it.
  - **Inadvertent disclosure to another authorized person within the entity:** physician participating in an organized health care arrangement.
  - **Recipient could not have reasonably retained the data:** explanation of benefits sent to the wrong individuals. Some of the EOBs are returned by the post office, unopened. Conclusion is that the information could not have been reasonably retained.

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).**

THE RISK ANALYSIS &

CULTIVATING A CULTURE OF COMPLIANCE

Leadership & A Culture of Compliance

"**Leadership** cultivates the foundation of **culture** to empower employees to achieve the **company** mission and realize how vital each of their contributions is to furthering those goals. **Leaders** have a responsibility to demonstrate the beliefs of the **company** and reinforce behaviors that reflect those values."

https://www.forbes.com/sites/williamcraig/2018/09/05/the-role-leadership-has-in-company-culture/#728b429316b6

"Take the Initiative"

- HHS-OIG Compliance Training
  - Cultivate a Culture of Compliance with Health Care Laws
    - Typically thought of as applying to Stark Law, AKS, FCA and Civil Monetary Penalties Law
    - https://oig.hhs.gov/compliance/provider-compliance-training/files/Provider-Compliance-Training-Presentationv2.pdf
  - Also applies to HIPAA and HITECH Act Compliance

Risk analysis requirement in § 164.308(a)(1)(ii)(A)

- Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.
- A risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.
- The National Institutes for Standards and Technology (NIST)
  - NIST, a federal agency, publishes freely available material in the public domain, including guidelines.
  - NIST provides guidance on evaluating and implementing various technical, administrative and physical safeguards.
- All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process.

https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

Audit Reports

- Statement on Standards for Attestation Engagements (SSAE) No. 18 (SSAE 18)
  - Effective May 1, 2017
  - Used in accordance with AICPA Service Organization Control (SOC)
- Statement on Standards for Attestation Engagements (SSAE) No. 16 (SSAE 16)
  - Introduced in April 2010 by the AICPA;
  - Supersedes the existing guidance (SAS 70) for performing an examination of a service organization's controls & processes;
  - Effective date of 15 June 2011.
  - Different types of SSAE 16 Reports
- International Standards on Assurance Engagements (ISAE) 3402

Privacy vs. Security

- Privacy Rule
  - Applies to all forms of PHI, including written and oral.
  - Applies to paper-to-paper faxes, video teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission.

- Security Rule
  - Standards and specifications of the Security Rule are specific to electronic protected health information (e-PHI).
  - E-PHI also includes telephone voice response and fax back up systems.

The Security Rule (6 main segments)

1. Security Standards: General Rules
2. Administrative Safeguards
3. Physical Safeguards
4. Technical Safeguards
5. Organizational Requirements
6. Policies and Procedures and Documentation Requirements

HIPAA & Cyber Training

"[T]he Security Rule simply establishes a floor, or minimum requirements, for the security of ePHI; entities are permitted (and encouraged) to implement additional and/or more stringent security measures above what they determine to be required by Security Rule standards."

TAP and Safeguards

- TAP = Technical, Administrative and Physical Requirements as set forth in CFR 164.302
- *Administrative safeguards* are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
- *Technical safeguards* means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

CFR 164.302)
TAP - Physical Safeguards v. Security Measures

- *Physical safeguards* are physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

- *Security or Security Measures* encompass all of the administrative, physical, and technical safeguards in an information system.

Technical Safeguards

- **Definition** – "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."
- Becoming more important because of the increased utilization of technology in health care, as well as ever changing advancements.
- **Examples**
  - **Access controls** provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions.
    - 1. Unique User Identification
    - 2. Emergency Access Procedure
    - 3. Automatic Logoff
    - 4. Encryption and Decryption

Administrative Safeguards

- **Definition** - "administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."
- **Examples**
  - Training
  - Designated Privacy/Security Officer
  - Sanction Policy
  - Policies and Procedures
  - Risk Assessment

Physical Safeguards

- **Definition** - "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- **Examples**
  - **Facility Access Control** - *"Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed."*
  - **Maintenance Records**
  - **Contingency Operations**

Security Incident Definition (CFR 164.302)

Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Cybersecurity

Cyber Security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

- Source: whatis.techtarget.com/definition/cybersecurity

The Fundamental Feature of Security…

- … is to protect the confidentiality, availability, and integrity of information and information systems.

Suggestions for Ensuring Privacy Compliance.

- Speaking quietly when discussing a patient's condition or information either in person or over the phone;
- Avoiding using patients' names in public areas;
- Double checking the information being discussed over the phone or being faxed, emailed or sent via mail. For example:
  - ✓ Is the address correct for the particular patient?
  - ✓ Is the information included that of the particular patient? and
  - ✓ Is the fax number correct?
- Posting signs to remind employees to protect patient confidentiality;
- Isolating or locking file cabinets or records rooms; and
- Providing additional security, such as passwords, on computers maintaining personal information.

Requirements Related to Cybersecurity Violations/ Attacks

- Accounting Standards Codification (ASC) 605-50 (during and after an incident) & 350-40 (before an incident)
- Diminished future cash flows
  - Potential impairment of goodwill, patents and capitalized software
- Disclosures to the SEC (Guidance Issued February 2018)
  - Material cybersecurity risks
  - Usually done on a Form 8-K or Form 6-K
  - https://www.sec.gov/rules/interp/2018/33-10459.pdf
- SEC Investigative Report Regarding Cyber-Related Frauds Perpetrated Against Public Companies & Related Internal Accounting Controls Requirements (October 2018)
  - Focus was the internal accounting controls, which are required under Sections 13(b)(2)(B)(i) and (iii) of the Exchange Act;
  - Specific focus was phishing and the perpetrators alleging to be either vendors or company executives; and
  - "Public issuers subject to the requirements of Section 13(b)(2)(B) must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures [as well as technical safeguards] accordingly."

CONCLUDING "NUGGETS"

Take-Aways and Questions

- A culture of compliance begins with an organization's leadership.
- Low-Hanging Fruit – Tips to Avoid Government Actions and Class Actions
  - Obtain the appropriate consent
  - Adequate training is essential
  - Complying with the required technical, administrative and physical safeguards is essential, in addition to adequate disclosure and obtaining the requisite consent of the affected individual.
- The Risk Analysis
  - Required under 45 C.F.R. § § 164.308(a)(1)(ii)(A).
  - Needs to be comprehensive and a SOC Report may not meet all of the requirements.
- Exceptions
  - Law enforcement

Thank You

Rachel V. Rose – Attorney at Law, PLLC

Houston, Texas

rvrose@rvrose.com

www.rvrose.com