

# Operationalizing HIPAA Compliance in a Rapidly Changing Global Regulatory Environment

March 2019

Pamela Hrubey, DrPH, CCEP, CIPP/US

# Topics for Discussion

---

- Operationalizing HIPAA in your organization
  - Key issues
  - Can Your Organization Pass Scrutiny? Key Steps to HIPAA Compliance
- The global privacy and data protection landscape





# Operationalizing HIPAA

## Key Issues

# Key Issues – Understand the Difference Between Required and Addressable

---

- Read the regulation (and read it again periodically) – items within are either *required* or *addressable*
  - **Required** - HIPAA specifies that the organization must implement the standard
  - **Addressable** – The organization is not required to implement the standard, but it is expected that the organization will give a reasonable explanation as to why a specific item is not necessary. Additionally, the organization must demonstrate other means of safeguarding data. Absent the additional step, the organization will be deemed to be in violation of the regulation
- If a requirement is addressable...it does NOT mean that the organization can ignore the need to establish a standard
- The organization is responsible to put other procedures in place that reasonably protect the personally identifiable information the corporation holds in a fashion that is consistent with their size, specific business purpose, etc.
- Once the organization has decided how to address specific items, it is important to document both the reasonable explanation and the procedures created to reasonably protect the personally identified information

# Key Issues – Policies and Procedures

---

- Policies and procedures are never really “done” - it is critically important as times and technology continue to change and privacy concerns grow, to implement the best practices into practice
- Many organizations adopt an annual update cycle for HIPAA-related policies and procedures each year...make it as easy as possible to remember this task by timing it to a specific date – the first month of the fiscal year, the first month of the calendar year, whatever makes most sense for your organization
- Consider leveraging a process that includes multiple authorized approvers by specific topic area to minimize the impact on the organization
  - Some organizations choose to use a SharePoint site or another readily accessible document repository for document sharing, review, and approvals



# Key Issues – Minimum Necessary

---

- Keep the minimum necessary requirement top of mind when dealing within the HIPAA sphere
- Avoid asking for or accepting more personally identifiable information than is necessary to complete the task at hand
- In particular, use the smallest amount of protected health information needed to accomplish the tasks associated with your job
- And, at the risk of sounding like the mistress of the obvious, if you don't need personal information (regardless of the type) to do your specific job, don't collect it and don't accept it
- Minimum necessary is also critically important in the area of technical safeguards needed
  - Limit access to information based on specific job requirements
  - Sometimes it is challenging to design and implement effective access controls that make sense to the organization (and that are actually efficient), but it is worth the effort because access controls can serve as an great “ring fence” preventing inappropriate access



# Key Issues - Encryption

---

- Encryption is considered a best practice / gold standard globally (regardless of the regulator)
- As such, encryption is likely to be one of the highest concerns an organization that processes protected health information should have
- This is listed in HIPAA as an addressable standard, so don't be misled into thinking it is ok to use a less rigorous approach to protecting personal information
- A common concern is the cost associated with implementing encryption
  - A fair argument especially for very small organizations (mom and pop shops)
  - That said, encryption provides such robust protection that it is challenging to figure out how to other address the standard in an acceptable fashion



# Key Issues – Business Associates

---

- As we have already discussed today...
  - A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
- Know who your business associates are, and get business associate agreements in place
- Follow up and make sure that your business associates understand what is expected of them and that they are actually following your standards
- Business associates need to meet all of your requirements for Administrative, Physical, and Technical Safeguards





# Key Issues – Data Integrity

---

- Consider what the organization is doing to make sure that the protected health information used by the organization has integrity (represents clinical reality)
- Consider how the organization will prove that personal information stored within servers and systems has not been altered inappropriately or inadvertently destroyed
- Electronic protected health information is extremely valuable...HIPAA places a large burden on the organization to make sure the data is protected and the only those who have access may view the information
- Having a secure environment for the data as well as the necessary firewall protection (and encryption) to protect data is vitally important

# Key Issues – Transmission Security

---


- While transmission security is a fairly simple concept, organizations often overlook this
- Organizations need to protect personal information to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network
- DO NOT EVER send electronic protected health information in a spreadsheet over email, through SMS text, etc.
- All data must be sent in a secure manner



# Key Issues – Workforce Training

---

- Avoid over-training...but simultaneously, don't under estimate the impact of well designed, memorable training for the entire workforce. Principles-based training can be short and to the point, and highly effective
- There will be some members of the workforce that need or would benefit from more specific training
- Remember to consider training needed after big events
  - Employee promotion
  - Employee job change
  - Addition of new contractor/vendor/third party/partner
  - Change in foundational or specialty platforms



# **Key Steps to HIPAA Compliance**

# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Assess and monitor Business Associate security and compliance programs—require each Business Associate to perform a privacy and security risk analysis on a regular basis and report results.



# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Maintain a current Business Associate Agreement with all Business Associates. Each Business Associate employee who handles protected health information must have a signed Business Associate Agreement on file.





# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Perform Security Risk Assessments on a regular basis and take corrective action. Any changes to PHI access triggers a new Security Risk Assessment. If a risk is identified, take corrective action immediately.



# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Implement technical safeguards focused on endpoint security software, user monitoring software, user controls, access controls and audit controls.



# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Ensure administrative safeguards through annual HIPAA training, employee testing and signatures on HIPAA acknowledgement agreements... “I have completed HIPAA training, understand the contents, and agree to abide by the related requirements”.



# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Follow all security safeguards and requirements, including...
  - Designate a security officer with written job description
  - Establish a security plan for laptops and remote access
  - Develop a thorough HIPAA security policy
  - Implement a security risk management program
  - Build a security breach incident response plan
  - Maintain six years of records on employees including background checks, validation of certifications and training, and annual list of excluded individuals and entities (LEIE) checks

# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Verify that your organization and your Business Associates have privacy safeguards in place
  - a designated privacy officer and job description,
  - privacy risk management plan,
  - HIPAA privacy plan,
  - privacy breach and incident response plan,
  - privacy plan for laptops and equipment,
- Electronic Protected Health Information policy to ensure transmission is secure and compliant,
- and off-boarding policies and procedures for terminating access to PHI when a workforce member terminates employment.



# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Guarantee physical safeguards to secure remote offices, employee equipment, phone conversations, and electronic documents and data displayed on an employee's workstation screen. Each employee should sign an acknowledgement statement to verify HIPAA compliance.





# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- It is prudent to have up-to-date photos of workspaces used by employees and Business Associates who work remotely. Best practice is to visit remote locations in person to verify compliance. OCR audits require proof that offsite and remote workspaces meet HIPAA compliance requirements.



# Tips for Ensuring Your Organization is in Compliance with HIPAA-related Requirements

---

- Finally, exercise extreme diligence with privacy and security rules if your organization uses offshore vendors to perform work and access protected health information. Legal teams should develop offshore vendor contracts that:
  - Hold the domestic Business Associate entity responsible for any breaches and any fines related to offshore breaches
  - Require the Business Associate to comply with all HIPAA requirements regardless of where work is performed
  - Require the Business Associate to maintain an appropriate level of insurance for cyberattacks, errors, omissions, etc. Follow up to check that that insurance is still in place.



# **Global Privacy and Data Protection Landscape**



# Evolution of Privacy and Data Protection – A Complex Environment

---

- Sweden, 11 May 1973 – First national-level data protection law designed to address the advent of computers processing personal data
- EU Data Protection Directive (95/46) 24 October 1995 – Expanded on the concepts put forward in Sweden
- Personal Information Protection and Electronic Documents Act (Canada) 1 January 2001 – Addressed commercial operations-related privacy concerns
- Health Information Portability and Accountability Act 14 April 2003 (United States, only addressing personal health data) – Addressed personal health information used for purposes of paying for healthcare
- HIPAA Security Rule 21 April 2005 (United States, only addressing security of health data)
- Global Data Protection Regulation (EU) 25 May 2018 – a brave new world
- California Consumer Privacy Act 1 January 2020 – a braver new world in a portion of the US
- General Data Protection Law (Brazil) Post 1 January 2020 – privacy protections expand in S.A.

# Overview of the General Data Protection Regulation – A New Global Standard?

## Accountability & Governance

Determining the organisation’s risk appetite in relation to data protection, enhancing accountability and governance through policies and standards that address the requirements of GDPR.

## Legal, Processes & Organisation

Establishing the legal basis for use, the Data Protection Officer’s role, handling data subjects’ requests, managing third parties, responding to data breaches, and implementing the supporting organisation, process and cultural changes.

## Information Security & Data Retention

Understanding and defining the approach to information security and personal data retention.

## Data Definition & Mapping

Understanding, defining and documenting the personal data that the organisation acquires and processes.

### RISK GOVERNANCE

(DP risk appetite and the link to wider Enterprise Risk Management framework)

### DATA GOVERNANCE

(ownership, stewardship and control of personal data acquired and processed)

### DP POLICY & STANDARDS

(enhanced policies and standards to govern the design of operational changes, in line with risk appetite)

### CONSENT, USE & LAWFULNESS OF PROCESSING

### DATA SUBJECT REQUESTS & RIGHTS

(SAR; RTBF; portability; restriction; rectification)

### THIRD PARTY MANAGEMENT

(legal docs; DD; oversight)

### BREACH MANAGEMENT & NOTIFICATION

### DATA PROTECTION OPERATING MODEL

(DPO role; privacy by design; DPIA; line 1 & 2 responsibilities)

### TRAINING AND AWARENESS

(delivery of enhanced DP training to meet needs, plus communications and culture change)

### INFORMATION SECURITY - ELECTRONIC

### INFORMATION SECURITY - PHYSICAL

### DATA RETENTION

(deletion; obfuscation; pseudonymisation)

### DATA DEFINITION AND MAPPING

(documenting and classifying uses, locations and internal/external movements of personal data)

**TRANSFERS OF PERSONAL DATA OUTSIDE EEA**  
(Standard Agreement; Binding Corporate Rules; Privacy Shield)



# More About the California Consumer Privacy Act of 2018

---

- **Effective sometime between 1 January 2020 and 1 July 2020**
- **What are the protections?**
  - The Act protects “personal information” which is defined as “any information that relates to a particular consumer or household.” The Act provides California residents the right to:
    - Request a record of what types of data, how it’s used, and who it’s shared with.
    - Full right of erasure
    - Object to the sale
    - Private cause of action for unauthorized access to non-encrypted or non-redacted personal information.

# The California Consumer Privacy Act of 2018

---

- **Who is protected?**

- Any “natural person who is a California resident.” Applies to “consumers” but also to patients, students, employees, etc.
- Does not apply to an individual who is in the state for a transitory purpose.

- **Which companies must comply?**

- A company must comply with the Act if any one of three conditions are present:
  - Annual gross revenues greater than \$25 million OR
  - Obtains personal information on 50k or more CA residents annually OR
  - 50% or more of the revenue comes from selling CA resident data
- Exception: A company may avoid complying if they do not have a
  - No Physical presence in or an affiliate in California AND
  - they can demonstrate that its “commercial conduct takes place wholly outside of California.”

# California Consumer Privacy Act of 2018

---

- **What are the requirements?**

- Companies must take proactive steps of compliance including (but not necessarily limited to):
  - Establish an ID verification process.
  - Provide data access requests method including a toll-free number.
  - Respond to data access requests within 45 days.
  - Disclose to whom they sell personal data and have in place a “Do Not Sell My Personal Information” button on their website home page. If an person opts out, do not contact for 1 year.
  - Obtain express opt in consent.
  - Avoid discrimination against a consumer based on the exercising of any of the rights granted in the bill.
  - Be able to offer higher tiers of services or products in exchange for more personal data if the exchange is not unjust or “usurious.”
  - Prepare data maps and inventories of personal information that document: locations of personal information, usage, and transfers.
  - Update privacy policies and disclosures to inform consumers of their rights.

- **And the specifics will change before the regulation goes “live” in 2020**

# Brazil Drives More Formally Into the Privacy and Data Protection Space With the New General Data Protection Law

---

- Replaces current sectoral legal framework which has been conflicting (and not widely enforced)
- Any practice that processes personal data will be subject to the law, subject to a few exceptions (areas like national and public security, pure research, artistic and journalistic purposes)
- Any foreign company that has at least an office in Brazil, or offers services to the Brazilian market and collects and treats personal data of data subjects located in the country, regardless of the nationality, will be subject to the new law.
- Very broad definition of personal data (includes data that when aggregated with other information might identify someone as “identifiable”)
- Includes a principle of accountability, which makes it mandatory for the data controller and data processor to demonstrate the adoption of effective measures capable of proving compliance with the rules for the protection of personal data (accomplished through a data protection assessment, may need to be transparent about the results)
- Must record all data processing activities
- Must take appropriate technical, security and administrative measures to protect personal data

# Change is Expected to Accelerate in the Privacy and Data Protection Space

---

- There has been a lot of change in a short time across the globe as it regards privacy and data protection
- This is expected to continue
- Stay tuned for more information on a U.S. Federal Privacy Regulation...dialogue is heating up (and all legislators, generally speaking, like to say they are interested in protecting the privacy of their constituents)
- Additional places where change is likely include
  - India
  - African continent
  - Asia Pacific (more enforcement is likely)





# Thank You

Pam Hrubey

Managing Director

Crowe LLP

317.208.1904

[Pam.Hrubey@Crowe.com](mailto:Pam.Hrubey@Crowe.com)