Regulations and Rules: Privacy Updates Impacting HIM

Rita K. Bowen, MA, RHIA, CHPS, CHPC, SSGB

Vice President, Privacy, Compliance and HIM Policy for MRO

MRO

Agenda

- Regulatory Updates
  - SAMHSA (42 CFR Part 2)
  - Global Data Privacy Rule (GDPR)
- Guidance
  - Disclosures for Emergency Preparedness
  - Cybersecurity and Ransomware
  - Texting in Healthcare
  - Opioids
  - HIPAA and Research
  - Patient Directed Requests
- Future Directives/Guidance
- Audience Questions and Discussion

Objectives

- Review recent regulatory updates and guidance impacting the privacy, security, and release of PHI to ensure organizational compliance
- Analyze issued guidance to foster successful implementation and management results
- Takeaway best practice tips for workforce education and training

Regulatory Update: SAMHSA

SAMHSA

New rule improves the exchange of medical information in ways that protect the privacy of people receiving substance use treatment

- The new rule is published in January 13th, 2017 - *Federal Register:* https://www.federalregister.gov/documents/2017/01/18/2017-00719/confidentiality-of-substance-use-disorder-patient-records

- The rules governing the confidentiality of substance use disorder records, often referred to as “Part 2”. In February 2016, HHS issued a notice of proposed rulemaking (NPRM) proposing changes to Part 2 to reflect the current health care delivery system

SAMHSA

Major Provisions Include:

- Will allow any lawful holder of patient identifying information to disclose Part 2 patient identifying information to qualified personnel for purposes of conducting scientific research if the researcher meets certain regulatory requirements. SAMHSA will continue to apply Part 2 rules when a program is federally assisted and holds itself out as providing substance use disorder diagnosis, treatment, or referral for treatment.

- Will allow a patient to consent to disclosing their information using a general designation to individual(s) and/or entity(-ies)(e.g., “my treating providers”) in certain circumstances. SAMHSA has added a requirement allowing patients who have agreed to the general disclosure designation, the option to receive a list of entities to whom their information has been disclosed to, if requested.

SAMHSA

Major Provisions Include:

- Has updated and modernized the rule to address both paper and electronic documentation

- **<u>Provisions being proposed include:</u>**
  - Clarifying and limiting circumstances in which disclosures to contractors, subcontractors and legal representatives of lawful holders may receive and utilize Part 2 data for purposes of carrying out the lawful holder's payment and health care operations activities
  - A new provision outlining CMS-regulated entities' (e.g., ACO's and QE's) use of contractors, subcontractors and legal representatives to carry out audit and evaluation activities that are necessary to meet the requirements of a CMS-regulated program

For more information, contact the SAMHSA Press Office at 240-276-2130.

Regulatory Update:
Global Data Privacy Rule (GDPR)

The GDPR

- A single, binding legislative act that reflects the implementation of the Unified Data Protection Strategy
- A complex regulation that may require significant changes in how you gather, use and manage data
- Imposes new rules on organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located
- Enhanced personal privacy rights
- Increased duty for protecting data
- Significant penalties for non-compliance

Global Data Privacy Rule (GDPR) – Defined

- The rule establishes a single set of rules for every EU member state to protect personal data

- What is "**Personal Data**"
  - Any information related to identifiable individuals or "data subjects"
  - Names
  - Credit card numbers
  - Emails
  - Government identification numbers
  - Health details
  - Online identifiers
  - Physical addresses
  - Real time coordinates generated by mobile devices

(this is not a finite listing)

GDPR – Effective Date

- **May 25, 2018-** into effect across Europe
- GDPR is the biggest overhaul of data protection laws in more than two decades

1. How prepared is your organization for GDPR?
2. How can your organization achieve compliance?
3. What steps should your organization take today to prepare for GDPR?
4. Other GDPR considerations?

GDPR – Applicable to…

- Businesses operating in the EU
- Those that process the data of people residing in the EU, no matter where the respective headquarters are located
- Any transfer of an EU citizen's personal data out of the EU into the U.S. must be done under an approved mechanism that protects the privacy and security of EU data
- Why should you be GDPR-compliant?

Guidance:
Disclosures for Emergency Preparedness

Disclosures for Emergency Preparedness

The storm hit – now what can we share?

- The Privacy Rule protects individually identifiable health information from unauthorized or impermissible uses and disclosures.
- The Rule is carefully designed to protect the privacy of health information, while allowing important health care communications to occur. This addresses the release of protected health information for planning or response activities in emergency situations.

- In addition, please view the Civil Rights Emergency Preparedness page to learn how nondiscrimination laws apply during an emergency.

  – https://www.hhs.gov/hipaa/for-professionals/special -topics/emergency-preparedness/index.html

Hurricane Irma – Preparation and Response

OCR Identifies Practices and Resources for Emergency Responders/Officials

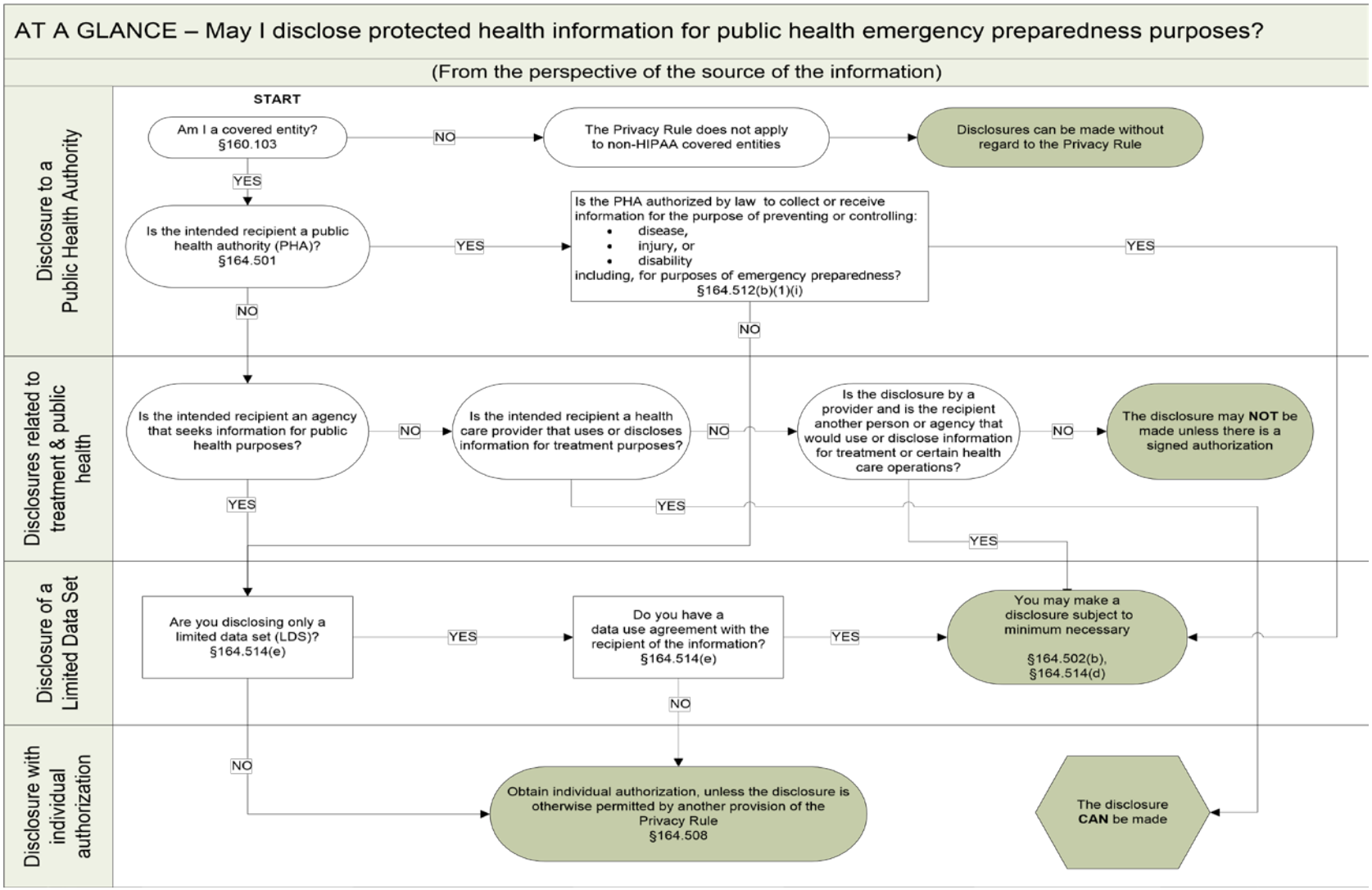
- For information about how HIPAA laws apply in an emergency

click here.

- Has a disaster been called?

- Basic information can be shared with family:
  - i.e. your location, etc.
  - Eliminates need to provide NPP –during disaster, but after disaster period then patients are to be provided the details
  - Basic information may be shared – but not healthcare details
  - You may share for public health activities

Disclosures for Emergency Preparedness



– https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/decision-tool-overview/index.html

Guidance:
Cybersecurity and Ransomware

Cyber and Ransomware

What is it?

- Result of attackers using email to trick users into clicking or opening messages that contain attachments with malicious code
- The infected machine gets most of its files encrypted, and then the key to decrypting the files is sold back to the user using bitcoin
- Users who have not backed up their data appropriately usually are forced to pay the ransom

Cyber and Ransomware

How was WannaCry different?

- It spreads at a faster rate
- Infection acted like a computer worm, scanning the computer or network for specific vulnerability and then infecting them
- The way it spread allowed for it to impact company servers and machines – and across the internet

Cyber and Ransomware

How do you prepare or combat?

- Risk Analyses vs. Gap Analyses
- Ongoing end-user training
  - Phishing
  - https://www.consumer.ftc.gov/media/game-0002-beware-spyware
- Appropriate and up to date patching
- Advanced security protection tools
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Cyber and Ransomware

Contingency Plan

- Disaster Recovery
- Emergency Mode or Continuity of Operations
- Data Backup

  – **KEY**

    1. Make it a policy and procedure

    2. Identify what is critical

    3. Operationalize and maintain the plan

https://www.phe.gov/Preparedness/planning/hpp/reports/Documents/hc-coop2-recovery.pdf

Cyber and Ransomware

We were attacked - what do we do now?

- Utilize HHS, OCR check list
  1. Execute your contingency plan
  2. Report the crime to law enforcement agencies
  3. Report breach to OCR

  Resources:
  - https://www.hhs.gov/sites/default/files/RansomewareFactSheet.pfg
  - https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to law-enforcement-officials/index.html

Cyber and Ransomware

AHIMA tools

- AHIMA releases 17 step Cybersecurity Plan
  - http://journal.ahima.org/wp-content/uploads/2017/12/AHIMA-Guidelines-Cybersecurity-Plan.pdg
    - REMEMBER – HEALTH RECORDS ARE SERIOUS BUSINESS FOR CYBER-CRIMINALS. ACCORDING TO IBM, HEALTH NOW TOPS THE LIST FOR THE MOST TARGEDED INDUSTRY FOR CYBERCRIMINALS
    - ON THE DARKNET HEALTH RECORDS NOW EXCEEDS $350.00 – WHILE CREDIT CARD INFO IS AT $2.00

Cyber and Ransomware

Summary

- Create a modern cybersecurity strategy
- Redouble efforts to secure mission-critical assets
- Apply environmental scans and conduct table top drills
- Develop an enterprise-wide culture of privacy and security
- Shift thinking from safeguarding applications to securing the data itself, regardless of how that data is received

  - **Key:**
    - PREPARE
    - DETECT
    - RESPOND
    - TRANSFORM

Guidance:
Texting in Healthcare

Texting of PHI

Can you or Can't you?

- To say that **texting** is in violation of HIPAA is not strictly true.
- **Texting** can be in compliance with HIPAA in certain circumstances depending on:
  - Content of the text message
  - Who the text message is being sent to
  - Mechanisms put in place to ensure the integrity of Protected Health Information (**PHI**)

- Is Texting in Violation of HIPAA? - HIPAA Journal
  - https://www.hipaajournal.com/texting-violation-hipaa/

Texting of PHI

How this creates problems in healthcare organizations

- Hard to control – with influx of “BYOD”
  - **80%** of medical professionals are using personal mobile devices
  - Most personal devices they are not employing log-in requirements
- The fines can be considerable

Texting of PHI

What is the solution?

- Secure Messaging
  - By encapsulating PHI within a private communication network that can only be accessed by authorized users
  - Access gained by secure messaging apps
  - With security mechanisms in place to prevent an accidental or malicious disclosure of PHI
  - It will not allow the user to
    - Send PHI outside of the communications network
    - Copy and Paste
    - Save it to an external hard drive
  - User is automatically logged off after a set period of inactivity

Guidance:
HIPAA and Responding to the Opioid Crisis

HIPAA and Responding to the Opioid Crisis

- HIPAA allows for the sharing of PHI in emergent and dangerous situations to family members/loved ones without patient permission
  - When incapacitated or unconscious
  - Serious/imminent threat to a patient's health/safety

- HIPAA limits the sharing of PHI with family/loved ones without patient permission if patient has capacity or limited capacity
  - Sharing not permitted
  - Must give patient opportunity to agree/object

HIPAA and Responding to the Opioid Crisis

- When decision-making capacity changes
  - Must offer patient opportunity to agree/object to further sharing
- Patient representatives still recognized by HIPAA and according to state law

If the Individual Is:	The Personal Representative Is:
Adult or Emancipated Minor	Examples: Health care power of attorney Court appointed legal guardian; general power of attorney or durable power of attorney that includes the power to make health care decisions Exceptions: abuse, neglect, and endangerment situations
Unemancipated Minor	Parent, guardian, or other person acting in loco parentis with legal authority to make health care decisions on behalf of a minor child Exceptions: abuse, neglect and endangerment situations
Deceased	A person with legal authority to act on behalf of the decedent or the estate Examples: executor or administrator of the estate, next of kin or other family member (if relevant law provides authority) Exceptions: abuse, neglect, and endangerment situations HIPAA defers to state law

Guidance:
HIPAA and Research

21st Century Cures Act and HIPAA Authorizations

- Requires HHS to issue guidance to help streamline authorization. Guidance must clarify the following:
  - (1) the circumstances under which the authorization for use and disclosure of PHI for future research purposes contains a sufficient description of the purpose of the use or disclosure
  - (2) the circumstances under which it is appropriate to provide an individual with an annual notice or reminder of the right to revoke an authorization
  - (3) appropriate mechanisms by which an individual may revoke an authorization for future research purposes

HIPAA and Individual Authorization of Uses and Disclosures of PHI for Research

- Guidance only applies to when an individual HIPAA authorization is obtained for uses and disclosures of PHI for research
- Requirements for valid HIPAA authorization still must be met (§164.508)
- Clarifies authorizations for future research must specify end date (i.e. “end of research study”)
- **Interim Guidance**
  - Not required if future studies not yet determined but should provide any intent
  - Provide patient sufficient “notice”

HIPAA and Individual Authorization of Uses and Disclosures of PHI for Research *(Continued...)*

- Revoked Authorizations
  - Applies the same as it does under HIPAA
  - May continue to use and disclose
    - Prior to the revocation
    - Maintain integrity of the research
    - Activities permitted already permitted under HIPAA
    - Re-disclosure by non-CE who received the information
  - Revocation statement must be included on authorization form including the process
    - May refer back to the Notice of Privacy Practice
    - Process should be outlined (i.e. electronic via portal or form)
      - Not burdensome or barrier to patient
  - Not effective till Covered Entity “knows”
  - May be oral (*not required*)

Remote Access Preparatory to Research

- Permitted with appropriate privacy and security safeguards
- Must comply with the Security Rule
  - Policies and Procedures
  - Encryption
- PHI not permitted to be removed from the Covered Entity at any time
  - Physically
  - Printing/Copying
  - Downloading/Saving
  - Faxing
  - Data Scraping
- Automatic download and temporary storage not permitted

Guidance:
Patient Right to Access

Patient Right to Access – Inspect & Copy

- Request should be in writing form/format
  - Authorization is not required
- Response should be within 30 days, unless state law mandates sooner
- Electronic requests – 3 business day norm
  - Maintained electronically
  - Designated record sets
- Charges – a reasonable cost based fee
  - Labor and the cost of supplies (Such As CD)
  - Postage
  - No retrieval fee

Patient Directed Request

(third parties)

- Must be in writing with patient's signature
- Clearly identify the designated recipient
- Clearly identify where to send the information

Patient Requests/Patient Directed Requests

Timing is critical

- Must be handled carefully with the highest priority

- May obtain or access information from the DRS
  - In the form and format that they are requested
  - For a reasonable, cost based fee
  - Within 30 days, of submitting the request

- A patient access request can be denied by a healthcare PROVIDER, but only if the provider determines that the disclosure could be harmful to the patient

Future Outlook

Future Outlook

- Enforcement of HIPAA by OCR
  - Restitution back to victims
- Consideration to remove Notice of Privacy Practice signature forms
- Good faith disclosures
  - First step: Opioid
- Accounting of Disclosures
- Guidance
  - Texting
  - Social Media
  - Encryption
  - Minimum Necessary
  - Breach Notice

Recommendations and Tips

- Create, Review & Update:
  - Policies and Procedures
- Workforce Education and Training
- Assess Overall Compliance
- Keep Current on Regulatory Forecast

Questions?

Contact Information

Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB

Vice President, Privacy, Compliance and HIM Policy

Email: rbowen@mrocorp.com

Office: 610-994-7500 x526

Cell: 813-503-3680

The views and opinions expressed in this presentation are those of the presenter and do not necessarily reflect or represent the views, opinions, or policies of MRO Corporation.

MRO