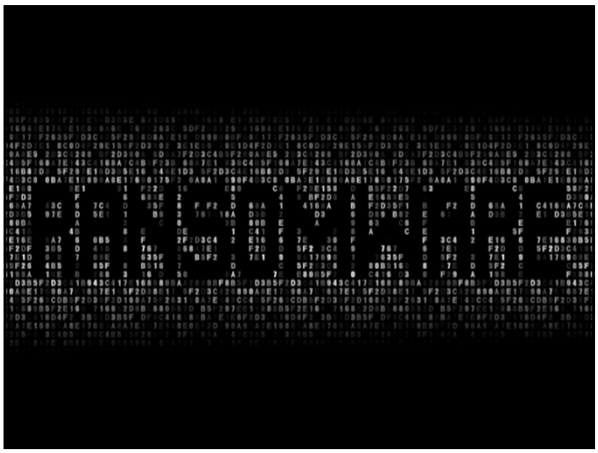

Ransomware and HIPAA

- When talking about how to prepare for and survive a ransomware attack, HIPAA provides a good blueprint
- If you have had a ransomware attack, you probably have also had a HIPAA breach

2

What is HIPAA? What is HITECH?

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Federal law to improve efficiency of health care industry
  - Privacy Rule (2003) and Security Rule (2005)
- The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
  - Focused on adoption of EHRs
- Final Omnibus Rule
  - January 2013; effective September 23, 2013 - sweeping changes

3

What is PHI?

Information that relates to:
(1) an individual's past, present, or future physical or mental health or condition,
(2) the provision of health care to the individual, OR
(3) the past, present, or future payment for the provision of health care to the individual

Covered Entities and Business Associates must vigorously protect against unauthorized use of or access to PHI that they create, receive, maintain, or transmit.

4

Who Must Comply with HIPAA's Requirements to Safeguard PHI?

- **Covered Entities** - Health plans, (e.g. Medicare or Medicaid) health care clearinghouses, and health care providers (doctors, nursing homes, or clinics) who bill electronically
- **Business Associates** - A person or entity that performs certain functions or activities for or on behalf of a covered entity that requires the person or entity to create, receive, maintain or transmit PHI. For example:
  - Law firms;
  - Billing/collection companies;
  - Financial institutions (other than pure banking services); and
  - Accounting firms
- **Subcontractors of Business Associates**

5

How HIPAA Compliance Can Help You **PREPARE** for and **RESPOND** to a Ransomware Attack – **SECURITY RULE**

- The Security Rule establishes national standards to protect electronic PHI. It requires entities to:
  - Implement security measures; and
  - Implement policies and procedures.

The HIPAA Security Rule could prevent the introduction of ransomware into your system and can help you respond to a ransomware attack!

6

How HIPAA Compliance Can Help You **PREPARE** for and **RESPOND** to a Ransomware Attack - **SECURITY RULE**

- **General requirements (45 C.F.R. § 164.306)**
  - Ensure confidentiality, integrity, and availability of electronic PHI created, received, maintained, or transmitted
  - Protect against reasonably anticipated threats or hazards to the security or integrity of such information
  - Protect against reasonably anticipated uses or disclosures of such information that are not permitted by the Security Rule
  - Ensure compliance by workforce
- **The Security Rule requires the implementation of certain safeguards:**
  - (1) administrative (45 C.F.R. § 164.308),
  - (2) physical (45 C.F.R. § 164.319), and
  - (3) technical (45 C.F.R. § 164.312)

7

How HIPAA Compliance Can Help You **PREPARE** for a Ransomware Attack

- **Security Management Process** (Administrative Safeguard)
  - Implement policies and procedures to prevent, detect, contain, and correct security violations
    - Risk Analysis
    - Risk Management Program
    - Sanction Policy
    - Information System Activity Review

8

How HIPAA Compliance Can Help You **PREPARE** for a Ransomware Attack – **RISK ANALYSIS**

- Assess risks and vulnerabilities to your information
- Methodologies vary depending on the size, complexities, and capabilities of your organization
- See HHS guidance regarding elements of a risk analysis: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

9

How HIPAA Compliance Can Help You **PREPARE** for a Ransomware Attack – **RISK ANALYSIS**

Elements of a Risk Analysis

1. Determine scope
2. Data collection
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation
9. Periodic review and updates

10

How HIPAA Compliance Can Help You **PREPARE** for a Ransomware Attack – **RISK MANAGEMENT PROGRAM**

- Composed of policies and procedures
- Your management and other key decision makers must be involved
- Prioritize risks that you identify from the risk analysis
- Determine options for mitigating the risks
- Develop a plan for implementing security measures
  - Security measures should guard against and detect malicious software

11

How HIPAA Compliance Can Help You **PREPARE** for and **RESPOND** to a Ransomware Attack – **EMPLOYEE TRAINING**

- Employees need to be trained on BOTH:
  - Threat of ransomware; AND
  - Policies/procedures to follow if they receive a ransom demand or believe the system has been infected
- Train and retrain employees
- Use simulated attacks

12

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **POLICIES**

What type of policies does your organization need?

- What to do when you find out you are being attacked;
- What actions you will take to get your data and your systems back; and
- Comprehensive data protection plan that meets your unique operational needs.

13

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **SECURITY INCIDENT POLICY**

HIPAA	RANSOMWARE
Identify and respond to suspected or known security incidents	Detect ransomware and conduct an initial analysis
Mitigate, to the extent practicable, the harmful effects of the security incident that are known	• Contain the impact and spread of the ransomware • Eradicate the instances of ransomware and remediate vulnerabilities that permitted the ransomware attack • Restore lost data and return to "business as usual" operations
Document security incidents and their outcomes	• Document attack and remediation • Conduct post-incident activities

14

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **EMERGENCY RESPONSE POLICY**

- Contact information for critical team members, federal authorities, and outside vendors (e.g. legal counsel and technical forensic investigators)
- Utilize decision trees
- Policies/procedures need to be tested and updated.

A timely response will limit damage.

15

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **CONTINGENCY PLAN**

Elements:

- Data Backup Plan
- Disaster Recovery Plan
- Emergency Mode Operation Plan

All contingency plans need to be tested and revised.

16

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **DATA BACK UP POLICY**

- All entities must have a data backup and recovery plan for all critical information
- Backup plans must include:
  - How often backing up
  - Where backing up
- Test backup plans

Ransomware attacks deny access to data. Maintaining frequent backups and ensuring the ability to recover data from backups is crucial to surviving a ransomware attack.

17

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **DISASTER RECOVERY POLICY**

- Document process to restore lost data and recover computer systems
- Define the resources, actions, tasks, and data required to manage the recovery process

18

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **EMERGENCY MODE OPERATION PLAN**

- Purpose: Enable the continuation of crucial business processes that protect the security of data during and immediately after a crisis situation

19

How HIPAA Compliance Can Help You **RESPOND** to a Ransomware Attack – **Security Rule Policies**

- **Workforce Security Policy**
- **Security Awareness and Training Policy**
- **Security Officer Policy**

20

HIPAA Breach

- Breach = the acquisition, access, use or disclosure of PHI in a manner not permissible under HIPAA which compromises the security or privacy of PHI
- If PHI is encrypted as part of ransomware attack, there has been an unauthorized disclosure
- Rule: An impermissible use or disclosure of PHI is presumed to be a breach, unless there is a *low probability* that the PHI has been compromised

21

Risk Assessment

Factors considered when conducting a risk assessment:

1. The nature and extent of the PHI involved;
2. The unauthorized person who had access to or used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated

22

HIPAA Reporting Requirements

Providing Notification To…	Breach Involved Fewer Than 500 Individuals	Breach Involved 500 or More Individuals
Individuals	No later than 60 days from discovery	No later than 60 days from discovery
U.S. Department of Health and Human Services	Submit a log of all breaches once a year, no later than 60 days after end of calendar year	At the same time as notice to individuals, no later than 60 days from discovery
Media	N/A	No later than 60 days from discovery

Chart comes from CMS Outreach and Education Materials
https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurityTextOnly.pdf

23