ENCRYPTION: ADDRESSABLE OR A DE FACTO REQUIREMENT?

Jonathan Carroll, MBA, CISSP
AVP – Enterprise IT Operations
Information Security Officer
University of Connecticut

Why Are We Talking About This?

- Data breaches in healthcare organizations are on the rise
  - Recent Ponemon study indicates that the frequency of data breaches has increased 32% from last year’s study
  - In addition, 96% of all healthcare providers have had at least 1 data breach in the last 2 years
    - 49% was a result of lost or stolen computing device

(Ponemon – Second Annual Benchmark Study on Patient Privacy and Data Security, December 2011)

Why Are We Talking About This?

- According to OCR, breaches involving more than 500 patients reached 400 and impacted over 19 million patients (as of 3/2/12).
- Twenty (20) breaches have accounted for the vast majority of affected patients (16+ million)
- There have been nearly 50,000 smaller breaches (<500 patients affected), since the Breach Notification Interim Final Rule
- Over 67,000 HIPAA complaints since reporting began in April 2003.

(HIPAA and Breach Enforcement Statistics – March 2012 – Health Information Privacy/Security Alert)

Walk Down Memory Lane
HIPAA Security Rule - April 2005

1. **HIPAA Standard 164.312(a)(1) Access Control**
   a. **Implementation Specification —** Encryption and decryption (A): Organizations must implement a mechanism to encrypt and decrypt ePHI.

2. **HIPAA Standard 164.312(e)(1) Transmission Security**
   b. **Implementation Specification –** Encryption (A) **:** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

HIPAA Security Rule

- So what does this mean?
  - The HIPAA Security Rule requires covered entities to safeguard electronic protected health information and permits them to use any security measures that allow them to reasonably and appropriately implement all safeguard requirements
  - HIPAA does not require encryption for all ePHI in all situations

What Should I Do…?

- A **required** implementation specification is similar to a standard, in that a covered entity must comply with it.
- For **addressable** implementation specifications, covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment.
  - In general, after performing the assessment, a covered entity decides if it will:
    - implement the addressable implementation specification
    - implement an equivalent alternative measure that allows the entity to comply with the standard; or
    - not implement the addressable specification or any alternative measures, if equivalent measures are not reasonable and appropriate within its environment.
  - Covered entities are required to document these assessments and all decisions.
- Remember, addressable does not equal optional!

Risk Assessment

- Encryption is an addressable implementation specification, meaning it is only required in areas deemed high risk by the organization's risk assessment.
- The output of a well documented risk assessment will result in an organization drawing their own defensible conclusions based on their own specific situation.
  - Although encryption is addressable, the decision not to encrypt in certain situations must be documented; failure to do sure could result in an audit finding of "willful neglect" and result in the levy of a monetary penalty
- Are people misinterpreting this? Perhaps….

Enter HITECH - 2009

- HITECH Breach Notification Interim Final Rule:
  - Notification in case of a breach (IFR issued 8/24/09)
  - Requires each individual to be notified if their “unsecured” protected health information is accessed, acquired or disclosed as a result of a breach

Unsecured PHI Defined

Section 13402(h)(1)(A) of the Act defines "unsecured protected health information" as protected health information that is not secured through the use of a technology or methodology that renders the information unusable, unreadable or indecipherable to unauthorized individuals.

Notification Requirements

- Obligation to notify patients without reasonable delay and no longer than 60 days
- If breach involves more than 500 people, then local media outlets need to be notified
- Severe monetary fines if found non-compliant
- Must attest annually to the Office of Civil Rights (OCR)
- Reporting is NOT optional
- OCR – "Wall of Shame"

A Critical Distinction

- Not all incidents are breaches, but all breaches begin as incidents:
  - A “security incident” is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PHI
  - A “breach” is the acquisition, access, use, disclosure of an individual’s PHI that poses a significant risk of financial, reputational or other harm

The Choice Is Yours

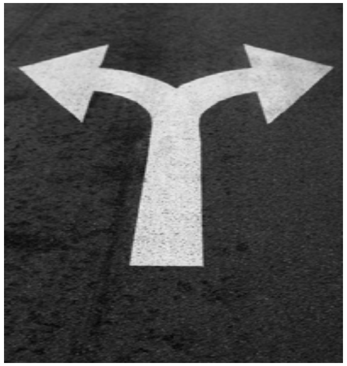
- Neither HIPAA, HITECH nor the Breach Notification Rule take away a Covered Entity’s flexibility in addressing how it safeguards protected health information. They simply clarify:
  - Breach of PHI without reasonable protection - HIPAA Security Rule issue
  - Breach of PHI without appropriate encryption - Notification issue

The Rules Have Not Changed

The Breach Notification Rule does not modify responsibilities under the HIPAA Security Rule nor does it impose new requirements to encrypt “all” protected health information. Entities are permitted to use “any” security measure that allows them to reasonably and appropriately implement safeguards.

Some Choices

- As required by the Act, the Secretary has published guidance relative to what makes protected health information unusable, unreadable and indecipherable:
  - Encryption
  - Destruction

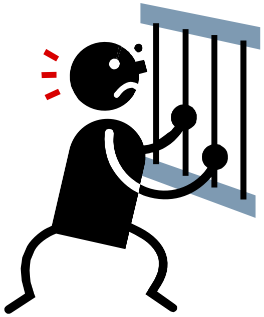


Avoid the Notification Issue

- So how do you make data unusable, unreadable and indecipherable to unauthorized individuals?

You ENCRYPT it!

- Safe Harbor -“Get out of Jail Free” card



Pay Me Now or Pay Me Later

- Cost of a Breach - Can you afford NOT to do it?
- Adopting encryption is a small price to pay to help ensure security, especially in light of the cost of reporting a breach.
- Latest information from Ponemon:
  - The latest U.S. Cost of a Data Breach report (3/8/11) shows costs continue to rise.
    - This year, they reached $214 per compromised record
  - Other notable items:
    - ***Rapid response to data breach costs more***. Companies that rushed to notify paid more
      - Are HITECH and all the state notification laws fueling over-notification?
      - What's the better scenario – rush through the notification process and risk losing more customers, or surgically examine the breach and notify fewer, at the potential risk of losing credibility for not notifying quickly enough?
    - Malicious or criminal attacks are causing more breaches
    - BUT negligence of employees still leads the way

Why Not "Pre" Breach?

- Post Breach Remedies from the 2010 Ponemon study:
  - Training and awareness was the overall #1 remedy
  - Encryption remains the most popular technology remedy
  - Other notable remediation procedures:
    - Additional manual procedures and controls
    - Identity and access management solutions
    - Data Loss Prevention (DLP) solutions

(2010 Annual Study: U.S. Cost of a Data Breach, Ponemon Institute)

De facto or Not…..

- Have HIPAA and HITECH really made encryption a de facto requirement?
- According to Wikipedia:

De facto (English pronunciation: /di□ □fæktoʊ/, /deɪ/[1]) is a Latin expression that means "concerning fact." In law, it often means "in practice but not necessarily ordained by law" or "in practice or actuality, but not officially established." It is commonly used in contrast to *de jure* (which means "concerning the law") when referring to matters of law, governance, or technique (such as standards) that are found in the common experience as created or developed without or contrary to a regulation. When discussing a legal situation, *de jure* designates what the law says, while *de facto* designates action of what happens in practice. It is analogous and similar to the expressions "for all intents and purposes" or "in fact.“

Doesn’t Look Like It…But It Ought to Be!

- If encryption is a de facto requirement – meaning “what’s happening in practice,” then the headlines, industry analysts and survey numbers don’t support this
- Breaches continue to make too many headlines….

Headlines - Hard To Ignore

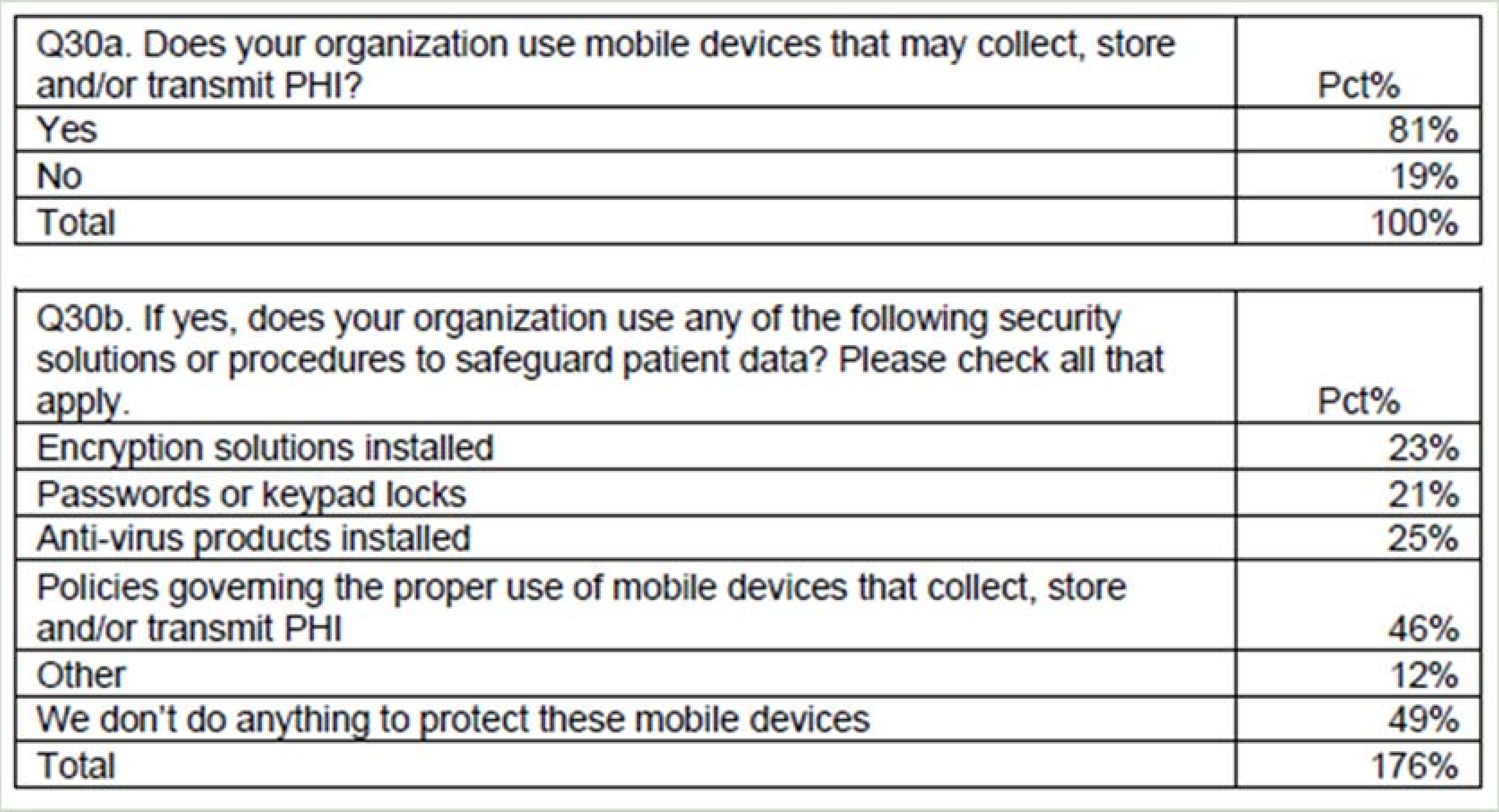
- “Medical Data Breaches Soar, According to Study” – CSO Magazine 12/1/11
- “Encryption and Other Database Security Lag at Healthcare Organizations” – Information Week Security 11/14/11
- “Electronic Medical Records Rarely Encrypted” – Reuters 11/9/11
- “Do As I Say…Not As I Oops!” – HipaaAudit.com 10/31/11
- And….any number of websites, blogs, etc. that track breaches such as OCR, The Breach Blog, DataLossDB, PrivacyRights.org

Recent HHS Guidance – 2/23/12

- In an attempt to eliminate the potential for patient data breaches on mobile devices, the Notice of Proposed Rule Making (NPRM) for Stage 2 Meaningful Use has proposed that mobile devices, including laptops, tablets, and smartphones that retain ePHI after a patient encounter should have default encryption enabled
- HHS IT Policy Committee has recommended that organizations take action to review encryption practices of ePHI as part of their risk analysis
- “There are certification requirements for electronic health records and we proposed that there be default encryption of data on end user devices, unless no data is kept after the session is ended on that user device.” – Dr. Farzad Mostashari, Head of ONC

(Information Week – 2/24/12)

2011 Ponemon Study



Q30a. Does your organization use mobile devices that may collect, store and/or transmit PHI?	Pct%
Yes	81%
No	19%
Total	100%

Q30b. If yes, does your organization use any of the following security solutions or procedures to safeguard patient data? Please check all that apply.	Pct%
Encryption solutions installed	23%
Passwords or keypad locks	21%
Anti-virus products installed	25%
Policies goveming the proper use of mobile devices that collect, store and/or transmit PHI	46%
Other	12%
We don't do anything to protect these mobile devices	49%
Total	176%

(Ponemon – Second Annual Benchmark Study on Patient Privacy and Data Security December 2011)

Easier Said Than Done

- Items to take into consideration:
  - Size, complexity and capabilities of your institution
  - Technical infrastructure, hardware and software security capabilities
  - Cost of security measures
  - The probability and criticality of risks to ePHI

Not a One Size Fits All

- Encryption comes in many shapes and sizes:
  - At Rest:
    - Hard drives, databases, copiers, etc.
  - In Motion:
    - Secure FTP (sftp)
    - Email
    - VPN or Citrix (ssl)
  - Mobile Devices/Portable:
    - Smart phones, tablets, USB drives
  - To further complicate this - Institutionally owned vs. personally owned devices

When To Encrypt – Some Guidance From Gartner

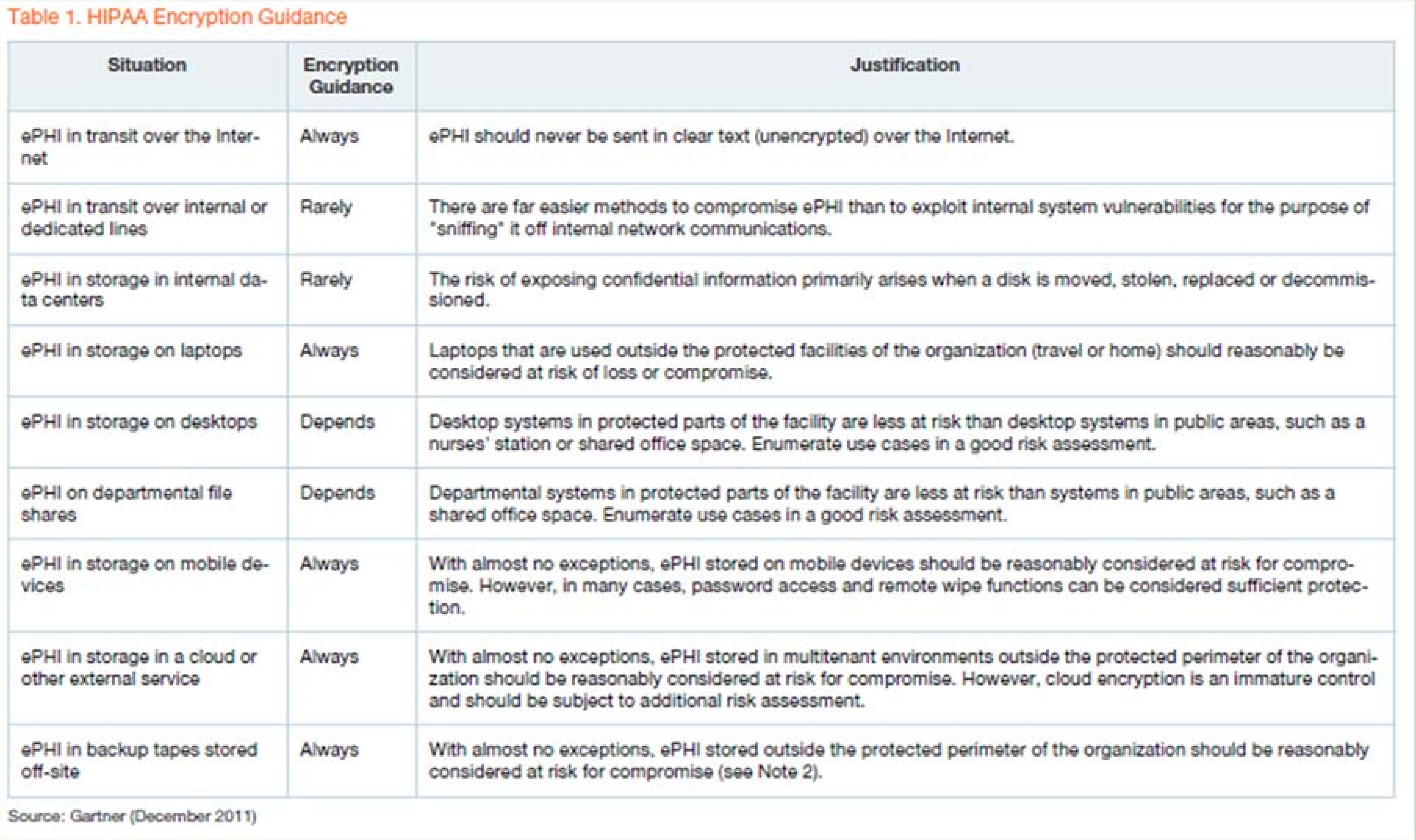


Table 1. HIPAA Encryption Guidance

Situation	Encryption Guidance	Justification
ePHI in transit over the Internet	Always	ePHI should never be sent in clear text (unencrypted) over the Internet.
ePHI in transit over internal or dedicated lines	Rarely	There are far easier methods to compromise ePHI than to exploit internal system vulnerabilities for the purpose of "sniffing" it off internal network communications.
ePHI in storage in internal data centers	Rarely	The risk of exposing confidential information primarily arises when a disk is moved, stolen, replaced or decommissioned.
ePHI in storage on laptops	Always	Laptops that are used outside the protected facilities of the organization (travel or home) should reasonably be considered at risk of loss or compromise.
ePHI in storage on desktops	Depends	Desktop systems in protected parts of the facility are less at risk than desktop systems in public areas, such as a nurses' station or shared office space. Enumerate use cases in a good risk assessment.
ePHI on departmental file shares	Depends	Departmental systems in protected parts of the facility are less at risk than systems in public areas, such as a shared office space. Enumerate use cases in a good risk assessment.
ePHI in storage on mobile devices	Always	With almost no exceptions, ePHI stored on mobile devices should be reasonably considered at risk for compromise. However, in many cases, password access and remote wipe functions can be considered sufficient protection.
ePHI in storage in a cloud or other external service	Always	With almost no exceptions, ePHI stored in multitenant environments outside the protected perimeter of the organization should be reasonably considered at risk for compromise. However, cloud encryption is an immature control and should be subject to additional risk assessment.
ePHI in backup tapes stored off-site	Always	With almost no exceptions, ePHI stored outside the protected perimeter of the organization should be reasonably considered at risk for compromise (see Note 2).

Source: Gartner (December 2011)

Issue Is Larger Than Just Encryption

- To be most effective, a Safe Harbor strategy needs to address more than just encryption
- Encryption should be one element of an "integrated" approach
- Encryption is not always the best or appropriate control
- Integrated approach should include elements such as……

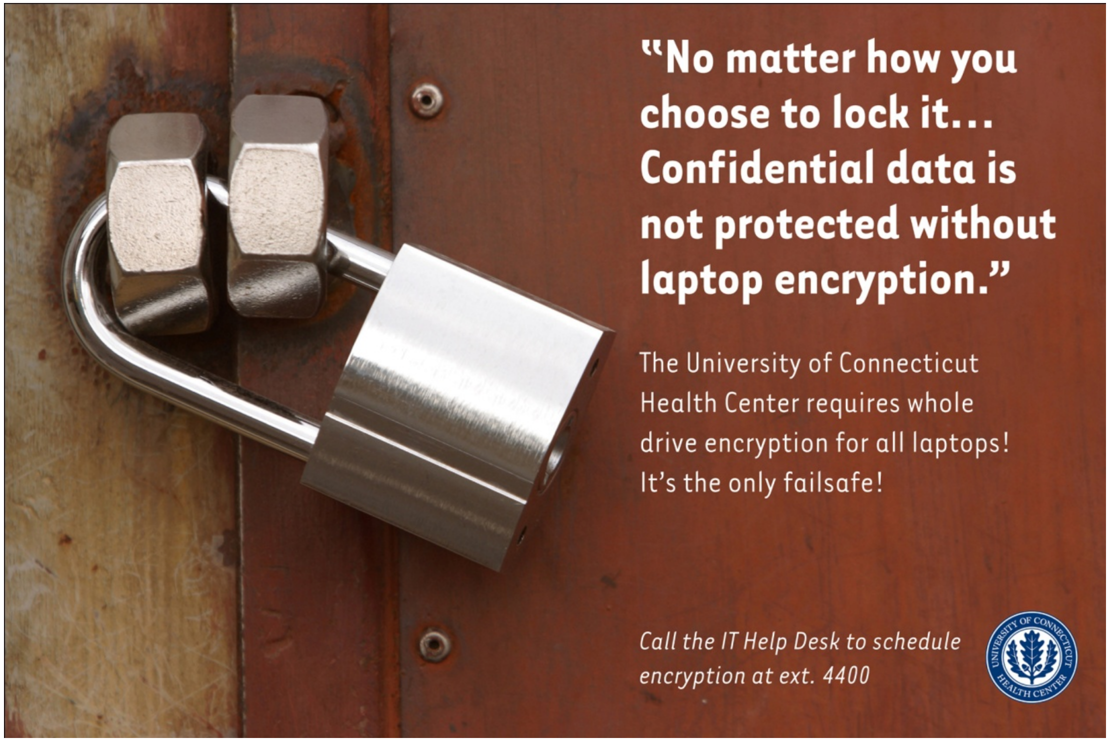
Integrated Approach

- Integrated approach should include elements such as:
  - Managing Patient Information Smartly
    - Know where your data is
  - Use Architecture To Isolate
    - Reduce or eliminate access to data sources; deploy separation in networks
  - Use Network Controls
    - Deploy Network Access Controls (NAC); conduct vulnerability tests and remediate

Integrated Approach (cont.)

- Implement Supplemental Technologies
  - Intrusion Detection, Data Loss Prevention, Security Event Information Management Systems (SEIM), firewalls, anti virus
- Don’t Forget About Physical Security
  - Physical controls including cameras, asset tracking, remote wipe options
- Turn on Auditing
  - Audit user actions, correlate information from SEIM system
- Security Awareness and Training
  - No technology is going to prevent users from being the weakest link

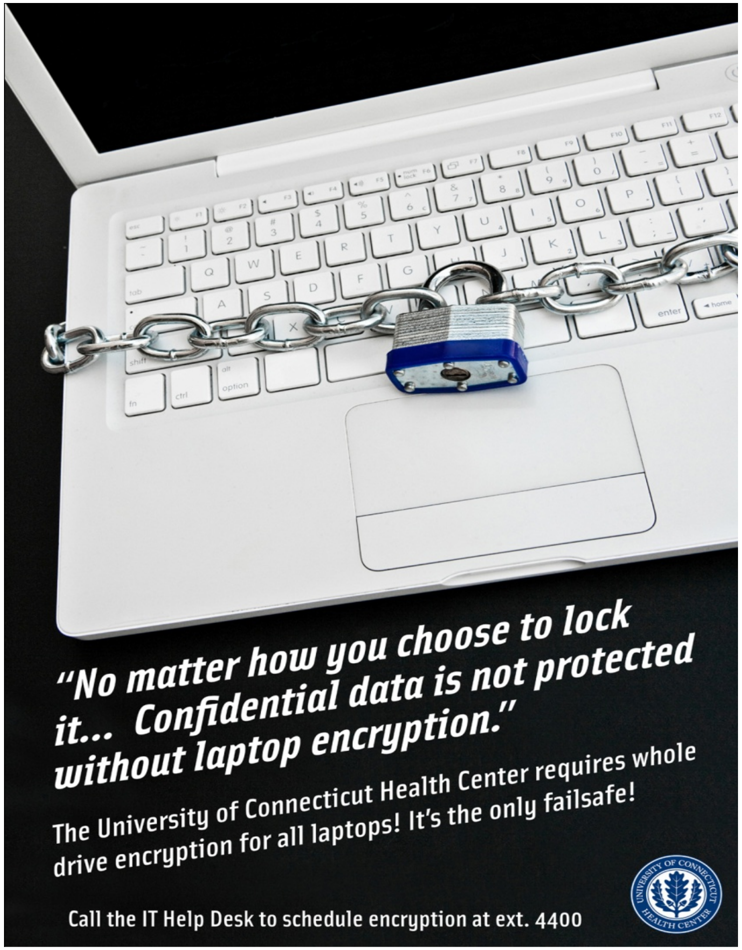
Encryption Awareness Campaign



"No matter how you choose to lock it… Confidential data is not protected without laptop encryption."

The University of Connecticut Health Center requires whole drive encryption for all laptops! It's the only failsafe!

Call the IT Help Desk to schedule encryption at ext. 4400



"No matter how you choose to lock it… Confidential data is not protected without laptop encryption."

The University of Connecticut Health Center requires whole drive encryption for all laptops! It's the only failsafe!

Call the IT Help Desk to schedule encryption at ext. 4400

Wrapping It Up

- Breaches continue to rise and make headlines
- HIPAA and HITECH are not prescriptive regulations; the rules have not changed since 2005; HITECH does not mean you must encrypt
- Encryption still remains “addressable” yet allows for “Safe Harbor”
- The cost of breaches/notifications continue to rise
- Device encryption is becoming a universal expectation (maybe after the fact by some organizations) and organizations need to consider it a de facto requirement where applicable
- Encryption is not a foolproof solution and must be part of a larger security program
- Organizations need to protect all sensitive information because it is the right thing to do!
- Public confidence will continue to suffer if organizations are not protecting their information
- The focus should be avoiding breaches

My Contact Info

Jonathan Carroll, MBA, CISSP
Assistant Vice President, Enterprise IT Operations
Information Security Officer
University of Connecticut Health Center
860-679-3528
jcarroll@uchc.edu