Encryption is Not Enough

2018 COMPLIANCE INSTITUTE

Andrew Rodriguez MSHI, HCISPP, CHPC, CHPS, CDP
Corporate Privacy and Information Security Officer, Shriners Hospitals for Children
Adjunct Instructor, University of Illinois at Chicago, College of Applied Health Sciences

Disclaimer

The information shared in this presentation is educational and does not constitute legal advices.

The views expressed here are solely those of the presenter in his private capacity and do not in any way represent the views of his employers.

Agenda

- Overview of Encryption Technology
- Lifecycle of Data and Information
- Breach Evaluation
  - Stolen/Lost Laptop or Desktop
  - Stolen/Lost Smart Phone
  - System or Application Breach
- Questions to Ask Your Information Security Officer

3

Overview of Encryption Technology

The Art of Encryption

Not the Science

4

What is Encryption?

UNENCRYPTED

The Red Wheelbarrow

so much depends
upon

a red wheel
barrow

glazed with rain
water

beside the white
chickens.

William Carlos Williams

ENCRYPTED

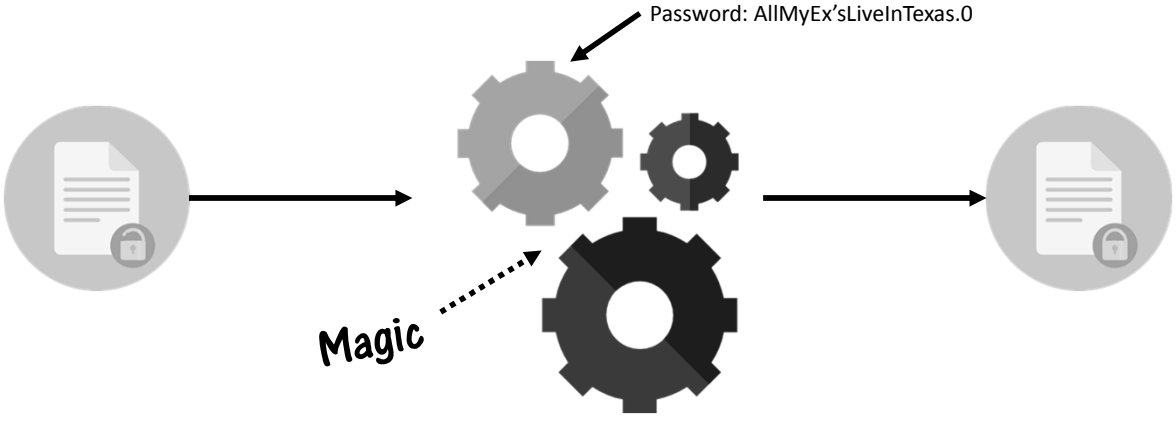
EnCt263d35ffeda3fd4e712bb4bc2bb3af87960cfbfb163
d35ffeda3fd4e712bb4bc2=yugUTxj9wLulhG9mlpB9Oe
XP5bmsQPlDr/s2L8YtPCheQkbGCMME7G5VKXEnoIhsP
BXv9oHpiMSnZVWMw3/gH74b6I0K6d+OXXVOrX19cu
wIL8qRuOck9Oj7yDsNe2qo/iCJZev7nDE+y8JVEZiayetIP
cFllQhckFHlM22irjjZyGb6S4facf/dNlXrS2ggHHotfrBe1o
=IwEmS

Decrypt it at https://encipher.it

Password: ThisIsMySuperSecretPassword!2017

5

What happens to the data?

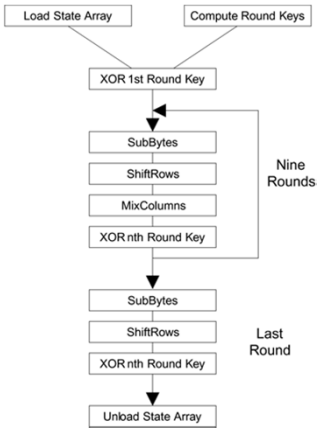


6

Not so magic, but out of scope

You take the following AES steps of encryption for a 128-bit block:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation.
- Copy the final state array out as the encrypted data (ciphertext).



7

Different types of encryption

THE GOOD

Advanced Encryption Standard (AES)

- Trusted standard in U.S.
- 128, 192, or 256-bits

RSA

- Standard used to send information over the Internet
- Uses private and public keys

Minor Players:

- Blowfish
- Twofish

THE BAD

Triple DES

THE UGLY

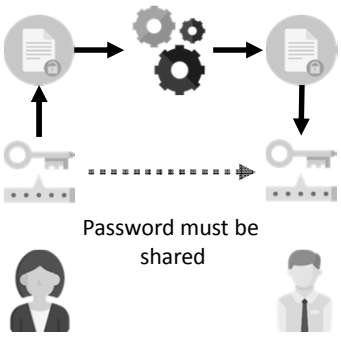
Custom Encryption

8

Basic concepts

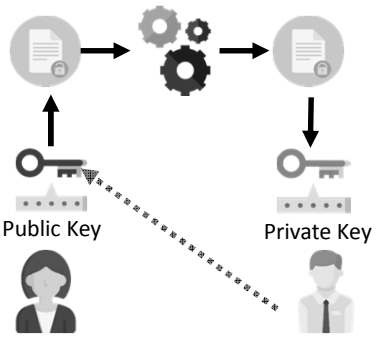
Symmetric Key Encryption

Secret Key



Asymmetric Encryption

Key pair

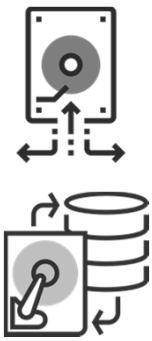


9

The things our data do…

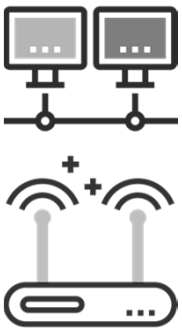
Data is plural for datum

DATA-AT-REST



Data that is persisted on storage, in a database, or archived on tape.

DATA-IN-MOTION



Data that is being transported between devices or on a network.

10

What a Privacy Officer needs to know

HIPAA SECURITY RULE

§164.312 Technical safeguards.

(iv) *Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

NIST PUBLICATIONS

Special Publication 800-111

Guide to Storage Encryption Technologies for End User Devices

References: *Federal Information Processing Standard (FIPS)*

https://www.hhs.gov/sites/default/files/nist800111.pdf

11

Lifecycle of Data and Information

From data to information

Data-at-Rest & Data-in-Motion

12

Data vs. Information

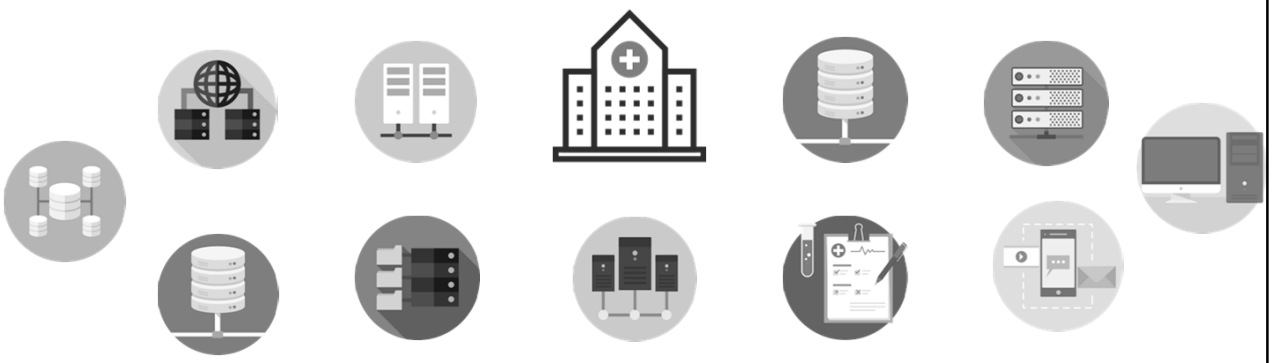
DATA	INFORMATION
Fact	Understanding from a collection of data points
Measurement	Data with context
Value	Data analyzed
Text	Data processed
Numbers	
Scores	
Date or Time	

13

P+HI = PHI

14

Where is your data?



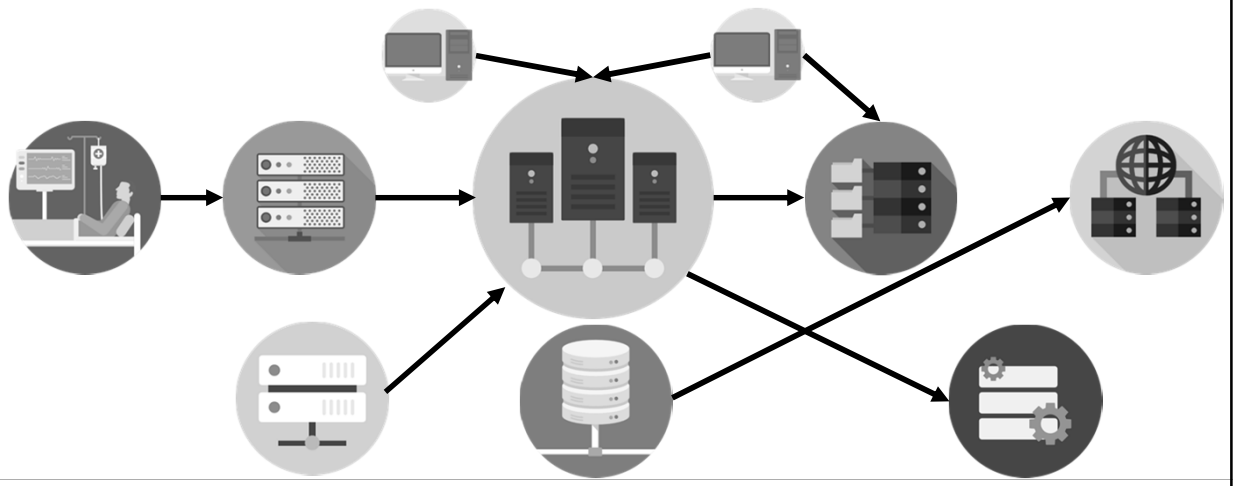
15

Where is your data?

- EHR/EMR
- File servers (reporting)
- File servers (photos)
- RIS & PACS
- Interface Servers
- Research Servers
- Smart Phones
- Cameras
- Patient Portal
- Physician Portal
- Report Server
- Email Server
- USB Drives
- Backup Tapes
- Fetal Monitoring Systems
- Lab Systems
- Pharmacy Systems
- Security Logs
- Data Warehouse
- Tele-Medicine
- Patient Education
- Patient Visitor Registration
- Practice Management
- Medical Devices
- Patient Monitoring
- Billing Systems
- Blood Bank Systems
- Cloud Services
  - Exercise Monitoring
  - Patient Tracking
  - Photo Editing
  - Backup Services
  - Document Management
  - Grammar Checker
  - Voice to Text
  - Reporting / Dashboard
  - Messaging
  - Email
  - Security

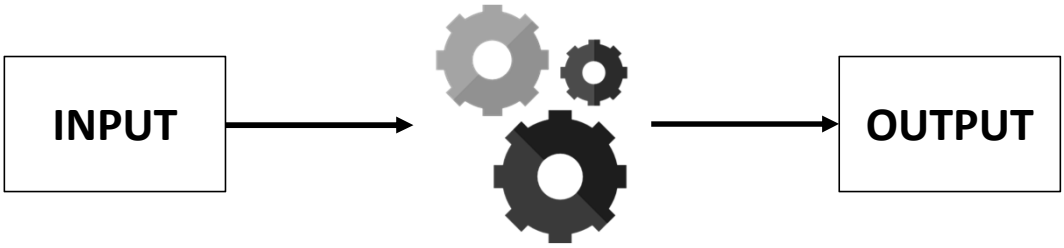
16

Complexity of Information



17

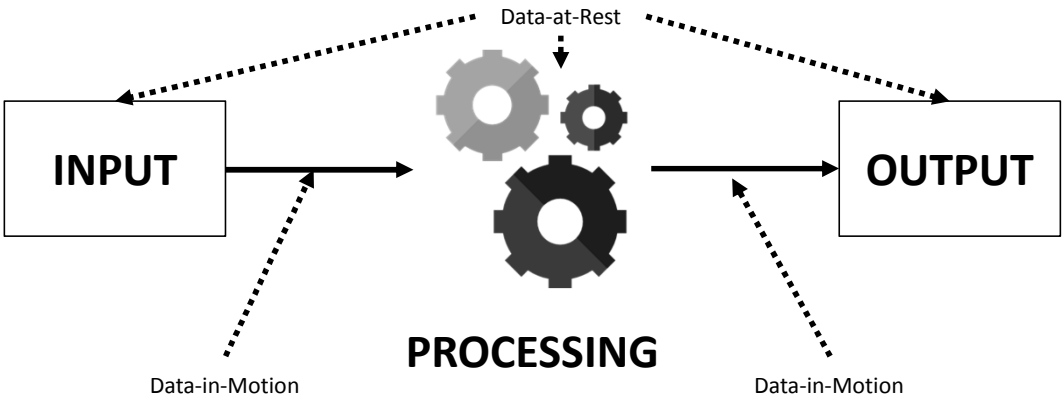
Data Distilled



PROCESSING

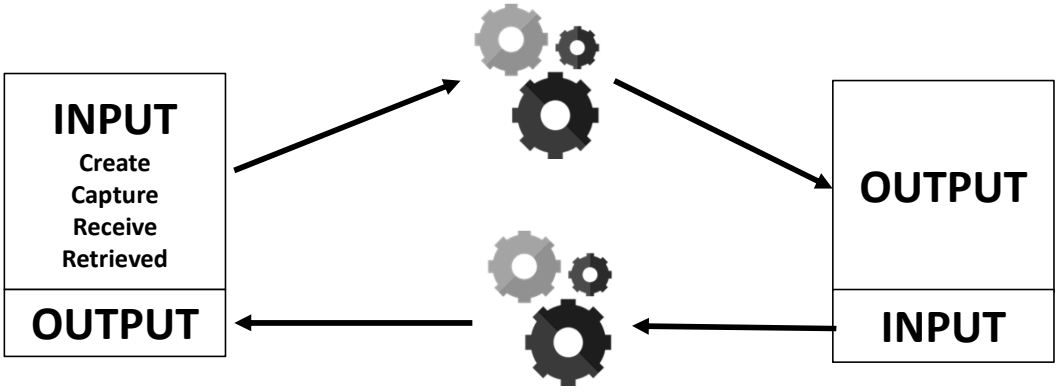
18

Data Distilled



19

Basic Information Lifecycle



20

Why this is important?

DATA-IN-MOTION

Best Practice:

- Encryption on protected networks
- Encryption to external networks

DATA-AT-REST

Best Practice:

- Encryption of disk (Server & SAN)
- Encryption of disk (workstations, laptops)
- Encryption of disk (USB, external HDD)
- Encryption of tape.

21

Breach Evaluation

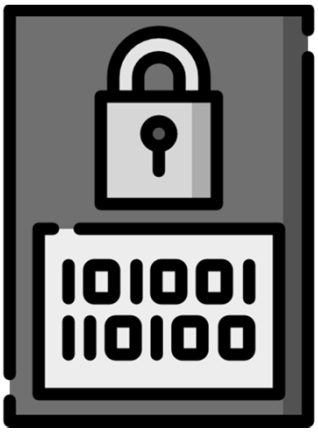
Beyond Encryption

22

Evaluation beyond encryption

If the information was encrypted, we are free from a breach, right?

Wrong!

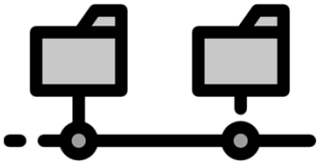


23

Breach: data-at-rest

Devices

Removable Storage



Files & Folders

Applications

24

Devices

What is the first (and sometimes only question) asked when a device is reported lost or stolen?

Is it encrypted?

25

Devices

If the answer is YES, then:

But what if….?

26

Devices

TECHNICAL

- Is there evidence that the laptop was encrypted?
- Was the laptop locked or powered off? Was it configured appropriately?
- What type of encryption? (Full-disk, or partial?)

PHYSICAL

- Was the user name and password with the laptop in written form?
- Were there any physical documents that were also stolen?
- Was removable media part with the device?

27

Devices

- Does the device backup to the cloud?
- Are there pictures of patients, medical images, or paper medical records?
- Is there evidence that the device was encrypted?
- Was the device backed up to a workstation at home or facility?
- If it is a BYOD (Bring Your Own Device) phone, when you open an attachment from an email does it store a copy of the file on the phone?

28

USB Storage

- Was the password with the device when lost or stolen?
- Is there evidence that the USB drive was encrypted?
- Do system policies allow a user to unencrypt devices?
- Do you keep an inventory of serial numbers for USB devices?

29

Files and Folders

- Are logs maintained on changes to access?
- Who had access at the time of the incident?
- Are logs maintained on who access files or folders containing PHI?
- Can files be exfiltrated via web-email, web-storage, or other cloud-based apps?

30

Systems

Encryption for data-at-rest helps if:

- The device is lost or stolen.
- Storage from the device is lost or stolen.
- Backup tapes are lost or stolen.

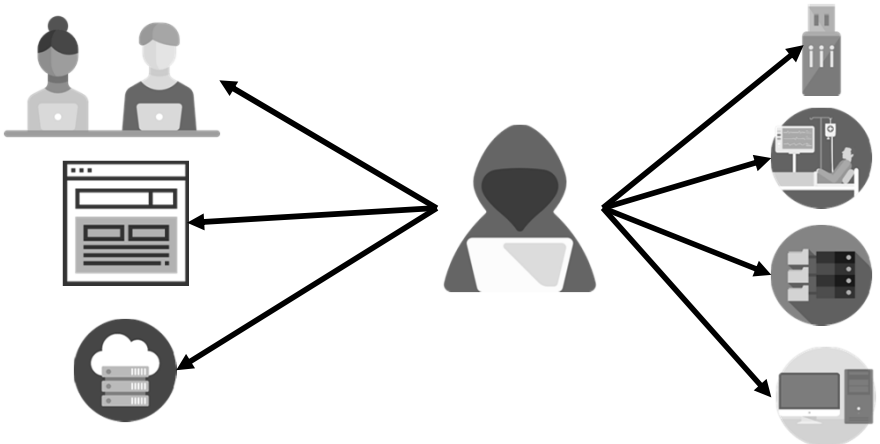
Encryption does not help for:

- Systems that are compromised.
- Accounts that are compromised.
- Devices that are compromised.

31

Attacks where encryption does not protect data

- Social engineering
- Web app vulnerabilities
- Vendor vulnerabilities
- Trojan devices
- IoT (Internet of Things)
- Compromised systems
- Compromised devices



32

Insider threat

Insider threats typically take longer to detect and are more difficult to detect.

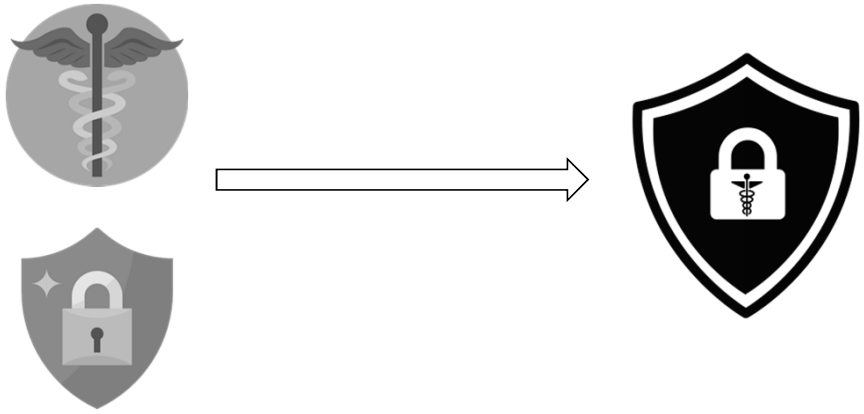
33

Questions to Ask Your Information Security Officer

And not make it look like you're getting into his/her business

34

Where Privacy & Security Intersect



35

How should the privacy and security officer interact?

PRIVACY OFFICER

SECURITY OFFICER

36

How should the privacy and security officer interact?

In healthcare, at the center of any information security / cybersecurity program **is privacy**.

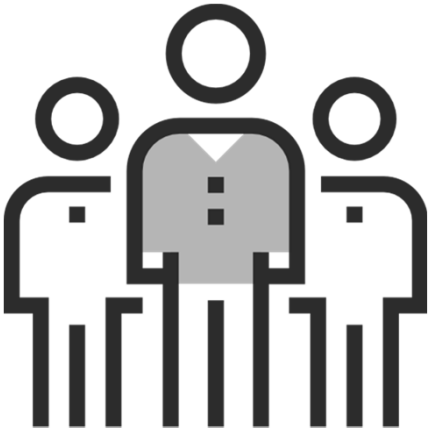
Privacy defines what we protect.

Security defines how we protect what we deem as private.

37

How well do security professionals know privacy?

- Protect the perimeter!
- Segregate the networks!
- Setup an IPS/IDS to monitor all subnets!
- Encrypt all drives!
- Backup all data!
- Monitor all logs!



38

Q1: Do you have an inventory of all data sets and repositories?

Often the focus is directed to the EHR/EMR system, mobile devices, and workstation encryption.

A comprehensive security program consists of all data sets and repositories.

Where is your data?

- EHR/EMR
- File servers (reporting)
- File servers (photos)
- RIS & PACS
- Interface Servers
- Research Servers
- Smart Phones
- Cameras
- Patient Portal
- Physician Portal
- Report Server
- Email Server
- USB Drives
- Backup Tapes
- Fetal Monitoring Systems
- Lab Systems
- Pharmacy Systems
- Security Logs
- Data Warehouse
- Tele-Medicine
- Patient Education
- Patient Visitor Registration
- Practice Management
- Medical Devices
- Patient Monitoring
- Billing Systems
- Blood Bank Systems
- Cloud Services
  - Exercise Monitoring
  - Patient Tracking
  - Photo Editing
  - Backup Services
  - Document Management
  - Grammar Checker
  - Voice to Text
  - Reporting / Dashboard
  - Messaging
  - Email
  - Security

39

Q2: Have you completed a risk assessment of all data sets and repositories?

Often the focus is directed to the EHR/EMR system, mobile devices, and workstation encryption.

A comprehensive security program consists of all data sets and repositories.

Where is your data?

- EHR/EMR
- File servers (reporting)
- File servers (photos)
- RIS & PACS
- Interface Servers
- Research Servers
- Smart Phones
- Cameras
- Patient Portal
- Physician Portal
- Report Server
- Email Server
- USB Drives
- Backup Tapes
- Fetal Monitoring Systems
- Lab Systems
- Pharmacy Systems
- Security Logs
- Data Warehouse
- Tele-Medicine
- Patient Education
- Patient Visitor Registration
- Practice Management
- Medical Devices
- Patient Monitoring
- Billing Systems
- Blood Bank Systems
- Cloud Services
  - Exercise Monitoring
  - Patient Tracking
  - Photo Editing
  - Backup Services
  - Document Management
  - Grammar Checker
  - Voice to Text
  - Reporting / Dashboard
  - Messaging
  - Email
  - Security

40

Q3: Are user access logs collected from all systems that involve PHI?

Focus tends to be only on the EHR.

Consider:

- File servers
- PACS
- Exercise equipment
- Cloud solutions

41

Q4: What strategies are in place for insider threats?

A few key strategies:

- Have a solid workforce off-boarding process.
- Have a solid workforce change/transfer process.
- Monitor all applications and repositories.
- Implement a Data-Identification solution.
- Implement a Data Loss Prevention solution.

42

Q5: Are folders provisioned by department or minimum necessary principle?

- By implementing a Data-Identification solution, you will be able to manage where data is stored without having direct access to the data.
- Audit department folders to ensure excessive access to PHI.
- Frequently audit organizational or “public” folders for PHI.

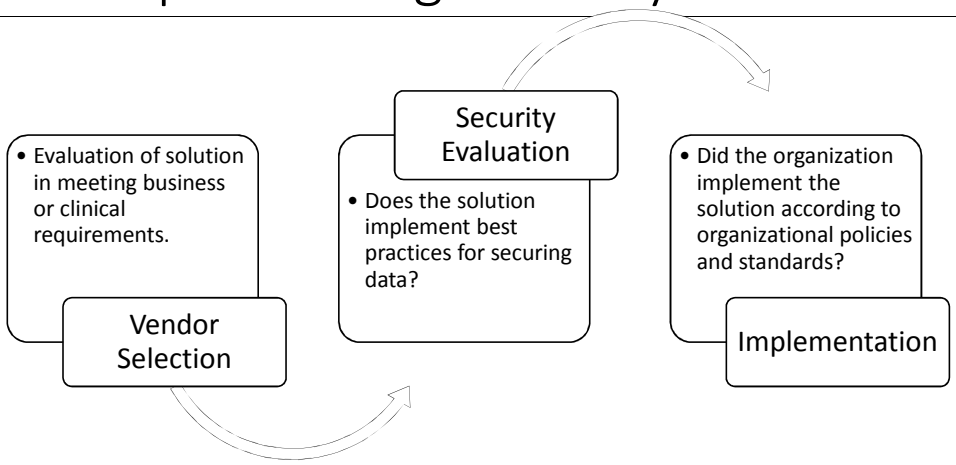
43

Q6: Do you retain evidence of encryption, access, or security changes?

- Inspect reports
  - There is a difference between:
    - “It was encrypted on 1/1/2015” and,
    - “Here is the automatic audit that shows it was encrypted the day it was lost”.
- Validate policy and procedures require devices and removable storage be encrypted prior to being used.
- Validate that reports or logs are available according to your organization’s retention policy.

44

Q7: Do you evaluate security controls after implementing a new system?



45

Q8: Can you provide access logs from reporting systems?

The best way to determine this is to walk backwards from a breach:

- A report containing appointment times, reason for appointment, and patient names is found on the Internet?
  - After inspecting the report, you can determine it is a report delivered to the ICU. The entire ICU department has access.
- Upon further research, you discover that it was an ad-hoc report.
  - From the logs, you know three ICU workforce members ran a report.
- Are you able to connect the report to who ran the report?

46

Q9: Do you have a security standard for the storage of reports & extracts?

Standards for reports and extracts would include:

- Authorized locations for storage
- Authorized means for transfer
- Required logging for transfer
- Appropriate use of reports & extracts
- Standards for including identifiers

Q10: Is the Privacy Officer notified when new systems are implemented?

MOST COMMON	BEST PRACTICE
The information security or cybersecurity team completes an assessment to determine the risk of information.	The information security or cybersecurity team completes an assessment to determine the risk of information.
Often, the focus is system specific.	The privacy team completes an assessment to determine the risk of information in the context of how workforce members use the system, how access is provisioned, and how information is used or disclosed.

Questions?

49

Contact Information

Andrew Rodriguez

Email: andrew@privacyinfosec.com

Privacy & InfoSec Resources: www.privacyinfosec.com

LinkedIn: https://www.linkedin.com/in/privacyinfosecofficer/

50