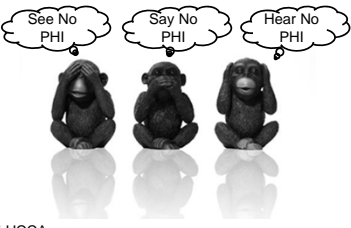




BREACH NOTIFICATION
Chris Duprey, Owner, Caris Consulting, LLC


Keeping Information Private

Confidential



Caris Consulting, LLC – 2015 HCCA

What happens when the "cat's out of the bag"?



Caris Consulting, LLC – 2015 HCCA

Definition of Breach

Breach

- Means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.
 - (i.e. stolen laptop)



Caris Consulting, LLC – 2015 HCCA

(1) Breach excludes:

- (i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.



Caris Consulting, LLC – 2015 HCCA

Exclusions, con't.

- (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
 - Files that were transferred to wrong individuals within the organization – wrong name selected on email list



Caris Consulting, LLC – 2015 HCCA

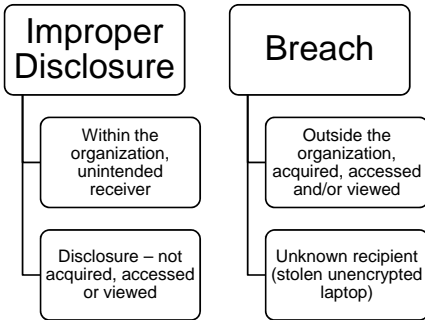
Exclusions, con't.



- (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Caris Consulting, LLC – 2015 HCCA

Unauthorized/Improper Disclosure vs. Breach



Breach Notification

The Final Rule was published on January 25, 2013 to be effective on March 23, 2013 with compliance required by September 23, 2013.

<p>In 1996 HIPAA did not require notification when patient PHI was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process.</p>	<p>In 2009 ARRA/HITECH <u>does</u> require notification of certain breaches of <u>unsecured PHI</u> to the following:</p> <ul style="list-style-type: none"> • Individuals • Department of Health and Human Services (HHS) • Media 	<p>On January 25, 2013, the Final Breach Notification Rule was published, requiring an entity to assess the probability that the protected health information has been or may be further compromised based on a risk assessment.</p>
---	---	--

Caris Consulting, LLC – 2015 HCCA

Application of Provisions and Penalties to Covered Entities

The diagram features a horizontal timeline with an arrow pointing to the right. Three vertical tick marks are labeled with the years 1996, 2009, and 2013. Below each year is a rectangular box containing text. The 1996 box states: 'CE responsible for BA, and subject to fines and penalties.' The 2009 box states: 'HITECH/ARRA penalties introduced by increasing the fines and levels of penalties.' The 2013 box states: 'Omnibus Rule- CE & BA responsible for the compliance and satisfactory assurances. Final modification which enhanced civil monetary penalties.'

Caris Consulting, LLC – 2015 HCCA

10

Penalty Considerations

- > Nature and extent of the violation
- > Nature and extent of the harm resulting from the violation
- > History or prior compliance with the administrative simplification provision, including violations by the covered entity or business associate, consideration of which may include but is not limited to:
 - Financial condition of the covered entity or business associate
 - Such other matters as justice may require

Caris Consulting, LLC – 2015 HCCA

11

Unsecure PHI

- > Unsecured PHI:
 - Means PHI that is not secured through the use of a technology or methodology specified by the "Guidance Specifying the Technologies and Methodologies that render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements Under HITECH/ARRA; Request for information".

Caris Consulting, LLC – 2015 HCCA


12

Compromising PHI Data

- Data in Motion – data that is moving through a network, including wireless transmission;
- Data at Rest – data that resides in databases, file systems, and other structured storage methods;
- Data in Use – data in the process of being created, retrieved, updated, or deleted; or
- Data Disposed – discarded paper records or recycled electronic media

Caris Consulting, LLC – 2015 HCCA 13

Have you implemented?



- > Encryption
 - Recommendations for the industry encryption standards to meet definition for "secured PHI"
- > Destruction
 - Recommendations for the industry destruction standards to meet the definition of "secured PHI"
- > Storage
 - Recommendations for the industry storage of electronic media to meet the definition of "secured PHI"

Caris Consulting, LLC – 2015 HCCA 14

Risk Factors to Consider for Breach Notification

An acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, **demonstrates that there is a low probability that the protected health information has been compromised** based on a risk assessment of at least the following factors:

- (1) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification
- (2) The unauthorized person who used the protected health information or to whom the disclosure was made
- (3) Whether the protected health information was actually acquired or viewed
- (4) The extent to which the risk to the protected health information has been mitigated

Caris Consulting, LLC – 2015 HCCA 15

Breach Discovery

- Discovery of an incident can be brought to your attention from internal systems or employees.
 - Ensure appropriate policies and procedures are in place to identify and report a potential incident for further investigation
- Clients or Patients can report an incident.
 - Ensure all information about the data is obtained from the initial report. How was the information acquired, accessed or viewed, who received the information and whether or not the original information can be retained.
- External, non-related entities.
 - Information that may have ended up at another organization but has been found or returned to the sender for further action.

Caris Consulting, LLC – 2015 HCCA

Breach Reporting

- Covered Entity/ Business Associate
 - Agreements will specify the time reporting requirements for unauthorized uses and disclosures, incidents and breaches;
 - Most agreements specify the information that is required within the report:
 - A brief description of what happened, date of the breach, date of the discovery;
 - Description of the types of unsecured PHI that were involved in the breach;
 - Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - Brief description of what the entity is doing to investigate the breach, to mitigate harm to individuals, and protect against future breaches; and
 - Contact procedures for individuals to ask questions or learn additional information pertaining to the incident
 - Reporting required to the covered entity no longer than 60 days from the date of discovery.

Caris Consulting, LLC – 2015 HCCA

Business Associate Impacts of Breach

Policies, procedures and training should be conducted to inform all employees handling e-PHI/PHI of the following breach tasks:

- Identification
- Investigation
- Report
- Supporting documentation
- Notification letter to the Covered Entity

Caris Consulting, LLC – 2015 HCCA

Breach Assessment

- Evaluating the Incident
 - Investigate the cause of the incident, define whether or not the incident is a breach by definition
 - Conduct the Breach Risk Assessment
 - Determine appropriate remediation
 - Notify appropriate individuals
- LoProCo – Low Probability that the data has been Compromised
 - The Breach Risk Assessment should be completed immediately to determine whether or not there is a low probability of compromise
 - If the conclusion is that there was a high probability of compromise – notification is required

Caris Consulting, LLC – 2015 HCCA

Breach Assessment

Factors	Low Probability	High Probability
The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification	Low probability that the information involved would identify who the individual(s) would be.	High Probability the individuals can be identified.
Who was the unauthorized person who received or accessed the PHI	Was the unauthorized individual an ee of the Covered Entity or another entity that is required to protect Privacy?	Was the recipient someone other than a covered entity or an employee of a similar entity?
Whether the PHI was actually acquired or viewed	Is there evidence that the information was not acquired or viewed?	Is it probable that the information was acquired and /or viewed? Is it unknown?
The extent to which the risk to the PHI has been mitigated	Were you able to get the PHI or make sure it was properly destroyed?	Were you unable to reduce the risk which in turn would contribute to more than a low probability that the PHI was compromised.

Caris Consulting, LLC – 2015 HCCA

Breach Notification

- Covered Entity – Plain language response
- Notification to Individuals
 - Written Notice (first-class mail / e-mail)
 - Substitute Notice (out-of-date contact information, <10 individuals alternative communication, >10 individuals conspicuous notice for 90 days on the home page of the website.
 - Additional Notice in Urgent Situations – phone or other means
- Notification to the Media
 - More than 500 residents of a State or jurisdiction, notify prominent media outlets serving the area;
 - Without reasonable delay no later than 60 days after date of discovery;
 - Content requirements remain the same.

Caris Consulting, LLC – 2015 HCCA

Breach Notification



• Notification to the Secretary

- Breaches involving 500 or more individuals, notification is required contemporaneously with the notice required to the individual and in the manner specified on the HHS Website.
- Breaches involving less than 500 must be logged and provided no later than 60 days after the end of each calendar year, report as required under the HHS Website.

To report a breach to the Secretary access this link:

- <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>

Caris Consulting, LLC – 2015 HCCA

Resolution Agreements

- [HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software](#)
- [\\$800,000 HIPAA Settlement in Medical Records Dumping Case](#) - June 23, 2014
- [Data Breach Results in \\$4.8 Million HIPAA Settlements](#) - May 7, 2014
- [Concentra Settles HIPAA Case for \\$1,725,220](#) - April 22, 2014
- [OCA Settles HIPAA Case for \\$250,000](#) - April 22, 2014
- [County Government Settles Potential HIPAA Violations](#) - March 7, 2014
- [Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts](#) - December 20, 2013
- [HHS Settles with Health Plan in Photocopier Breach Case](#) - August 14, 2013
- [WellPoint Settles HIPAA Security Case for \\$1,700,000](#) - July 11, 2013
- [Shasta Regional Medical Center Settles HIPAA Privacy Case for \\$275,000](#) - June 13, 2013
- [Idaho State University Settles HIPAA Security Case for \\$400,000](#) - May 21, 2013

Caris Consulting, LLC – 2015 HCCA

Summary




- Analyze the incident against the definition of a breach
- Determine if it is a breach or unauthorized disclosure
- Investigate the incident, how many individuals are affected, why it happened, what can be done to prevent it in the future
- Conduct the Breach Risk Assessment
- Determine whether or not there is a Low Probability of Compromise or High Probability of Compromise
- Notify appropriate individuals

Caris Consulting, LLC – 2015 HCCA


Un-Tech Your Tech:
A non-technical overview of Technical Safeguards, including network and end point security, describing available technology options for organizations of various sizes, to meet requirements.

AMIT KULKARNI,
CEO, Secure Healing Inc.
amit@securehealing.com


Secure Healing  25


Agenda

- The need of Security
- Information Security – Basics
- Securing Data – The ignored kind
- Recommended Open Source products

Secure Healing  26

Everything is networked



Secure Healing  27

DATA BREACHES ARE TOP OF MIND FOR HEALTHCARE ORGANIZATIONS

Back Street: Employees with access to data breach suit for Sun Lane

Cadence-Sent care number of patient files in data breach much higher

Community Health Systems Says Data Breach Data Action

Secure Healing 28

CURRENT PRIVACY BREACH INVESTIGATIONS ARE RETROACTIVE

1. Patient/Employee/IT gets suspicious of unknown access
2. Complaint to Security/Privacy Officer
3. They log into Multiple reporting solutions
4. Try to correlate data from various sources
5. IT Security/ HR will stop bad guy's access/ give disciplinary action to user (insider)

Secure Healing 29

ROGUE USERS CAN EASILY AVOID DETECTION


1. Internal user or malicious outsider accesses data and is careful to not disclose to others
2. No Alerts
3. No Investigation
4. No one gets caught

Secure Healing 30

The Threat


- Cyber Criminals - (financial data)
- Cyber-warriors - (political/military)
- Corporate espionage - (IP theft)

- Hacktivists - (idealism)
- Individual Hackers - (fame/thrill)
- Spammers - (ad distribution)


Secure Healing  31

Covert Channels

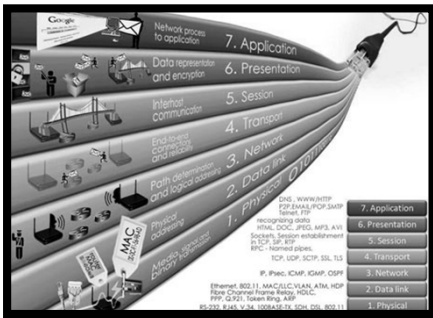
- Clever misuse of network protocols
- Nearly undetectable
- Not that uncommon




“They’ ll never see me coming!”

Secure Healing  32

The Basics - The OSI layers



Secure Healing  33

The Basics - Security Controls

Source: Spring 2013 SANS Poster

Secure Healing 34

Enterprise Security's Gaping Hole

"64% of the 10 million security incidents tracked targeted applications."
Information Week

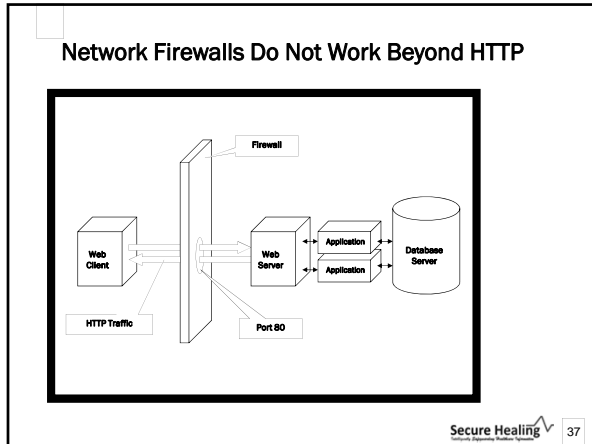
Secure Healing 35

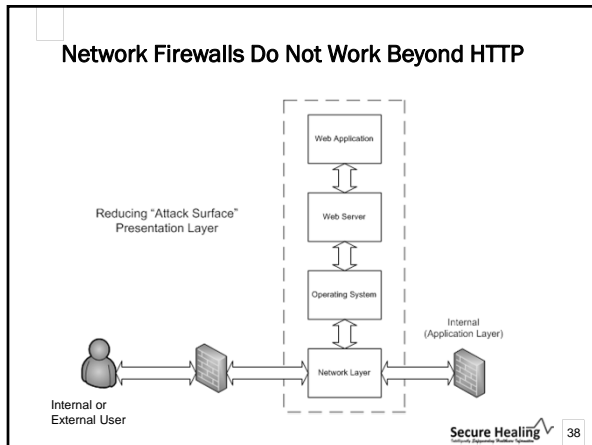
Why Should I Care?

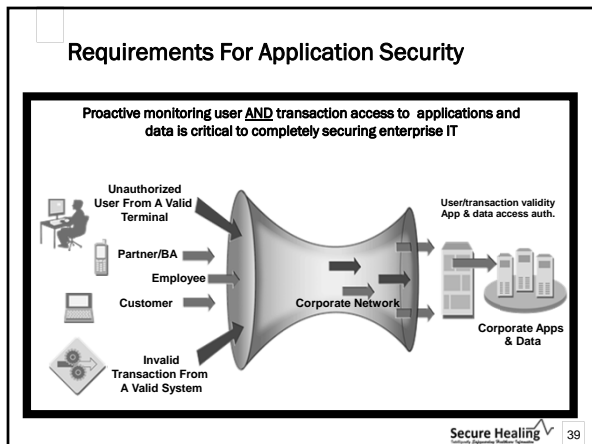
Let's just think this through...

- **How likely is a successful web application attack?**
 - Stunningly prevalent .. check the recent breach headlines
 - Easy to exploit without special tools or knowledge
 - Little chance of being detected
- **Consequences?**
 - Disclosure of database contents
 - Loss of authentication and access control for users
 - Defacement
 - Secondary attacks from your organization

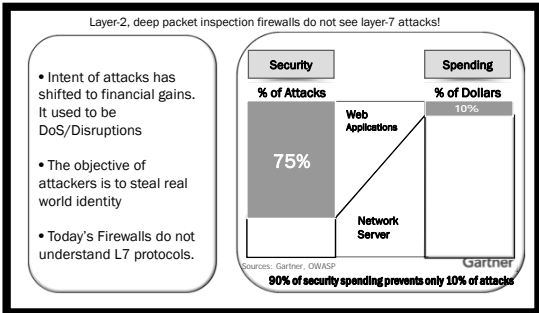
Secure Healing 36







Why Another Security layer?



- Intent of attacks has shifted to financial gains. It used to be DoS/Disruptions
- The objective of attackers is to steal real world identity
- Today's Firewalls do not understand L7 protocols.

Monitoring

- Use IDS/IDP
- Offload logs to central repository
- Custom apps need to generate logs
- Understand what's going on - situational awareness

Sniffing

A sniffer is a program that monitors and analyzes network traffic and is used legitimately or illegitimately to capture data transmitted on a network

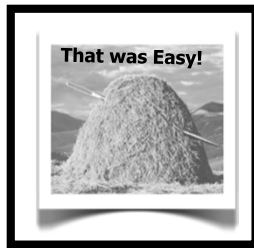


Defense-In-Depth

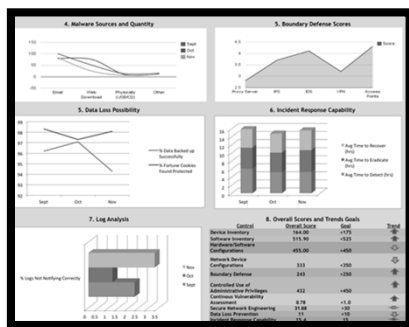
- Defense-in-depth is an information assurance (IA) strategy in which multiple layers of defense are placed throughout an information technology (IT) system.
- It addresses security vulnerabilities in personnel, technology and operations for the duration of the system's life cycle.

Defensive practices

- Firewall
 - Block outgoing unexpected ICMP or non-needed traffic
- Intrusion Detection
 - Spotting known signatures
- Anomaly Detection
 - Spot unusual spikes in traffic/access
 - Any anomalous behavior (How hard is that?!)
- Disk Encryption
 - Does it stop malicious users/hackers ?

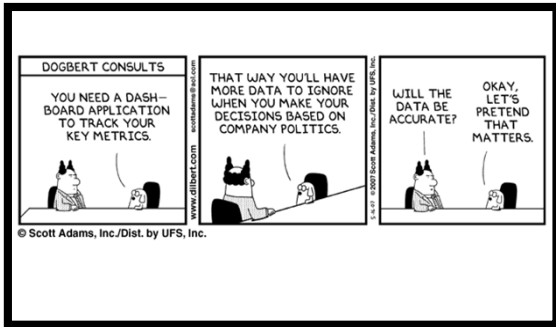


Visualization / Dashboard



Source - SANS Technology Institute

Visualization / Dashboard



Summary


- Assume you will be targeted/hacked/breached by a rogue insider or malicious outsider
- Defenders need to look for indicators of compromise across many sources
- SIEM solution centralize data
- Start small with basic methods, test, and move to more advanced techniques
- Goal is to detect breach as early as possible and gather as much information as possible before starting incident response

References

- Twenty Critical Security Controls for Cyber Defense: SANS/CAG
- Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous FISMA Compliance by John Gilligan
- Security Metrics, Replacing Fear, Uncertainty and Doubt, Gary McGraw
- A Guide to Security Metrics (SANS Reading Room), Shirley C. Payne
- NIST Guides to Security
<http://csrc.nist.gov/publications/PubsSPs.html>

Some New Open Source Security Products

1. **Truecrypt:** - encrypt all the things.
2. **Suricata:** leverages both signature and anomaly-based intrusion detection.
3. **GRR Rapid Response:** An open source incident response tool currently in beta.
4. **The Sleuth Kit:** The Sleuth Kit features a library and a collection of tools for investigating disk images, including volume and file system data.

Secure Healing  49

Thank you !

AMIT KULKARNI,
CEO, SECURE HEALING Inc.


amit@securehealing.com
Stop by at HCCA conference booth # 605

Secure Healing  50


BAKER TILLY
Candor. Insight. Results.


**Senior Manager, Baker Tilly Virchow
Krause, LLP**
Daniel.Steiner@bakertilly.com

Physical Safeguards


Candor. Insight. Results.

PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		
Workstation Security	164.310(c)		
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)


Physical Safeguards – Facility Access Controls


Candor. Insight. Results.


Contingency Operations (Addressable) - Physical security measures entities established in the event of the activation of contingency plans and employ while the contingency plans required by the Administrative Safeguards are active.

Sample questions to ask:

- Are procedures developed to allow facility access while restoring lost data in an emergency?
- Can the procedures be appropriately implemented by workforce members responsible for the data restoration process?
- Do the procedures identify personnel that are allowed to re-enter the facility to perform data restoration?



Physical Safeguards – Facility Access Controls


Candor. Insight. Results.


Facility Security Plan - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

1. Locked doors, signs warning of restricted areas, surveillance cameras, alarms.
2. Property controls such as property control tags, engraving on equipment.
3. Personnel controls such as identification badges, visitor badges and/or escorts for large offices.
4. Private security service or patrol for the facility.

Sample questions to ask:

- Are policies and procedures developed to protect the facility and associated equipment against unauthorized physical access, tampering, and theft?
- Do the policies and procedures identify controls to prevent unauthorized physical access, tampering, and theft?


Physical Safeguards – Facility Access Controls


Candor. Insight. Results.


Access Control & Validation Procedures - Implement procedures to control and validate a person's access to facilities based on their role or function.

Sample questions to ask:

- Are procedures developed to control and validate a person's access to facilities based on their role or function?
- Do the procedures also identify visitor controls, such as requiring them to sign in, wear visitor badges and be escorted by an authorized person?




Physical Safeguards – Facilities Access Controls


Candor. Insight. Results.


Maintenance Records - Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks).

Sample questions to ask:

- Are policies and procedures developed and implemented that specify how to document repairs and modifications to the physical components of a facility which are related to security?
- Do the policies and procedures specify all physical security components that require documentation?



Physical Safeguards – Workstation Use



Candor. Insight. Results.

Workstation Use - A workstation is defined as an electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Sample questions to ask:

- Are policies and procedures developed that specify the proper functions to be performed, the manner in which they are performed, and the physical attributes of the surroundings of a specific workstation that can access ePHI?
- Do the policies and procedures identify workstations that access ePHI and those that do not?
- Do the policies and procedures specify the use of additional security measures to protect workstations with ePHI, such as using privacy screens, enabling password protected screen savers or logging off the workstation?

Physical Safeguards – Workstation Security



Candor. Insight. Results.

Workstation Security - Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

Sample questions to ask:

- Are physical safeguards implemented for all workstations that access ePHI, to restrict access to authorized users?
- Have all types of workstations that access ePHI been identified, such as laptops, desktop computers, personal digital assistants (PDAs)?
- Are current physical safeguards used to protect workstations with ePHI effective?


Physical Safeguards – Device and Media Controls


Candor. Insight. Results.


Device and Media Controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility.

Sample questions to ask:

- Are policies and procedures developed and implemented that govern the receipt and removal of hardware and electronic media that contain ePHI, into and out of a facility, and the movement of these items within the facility?
- Do the policies and procedures identify the types of hardware and electronic media that must be tracked?




Physical Safeguards – Disposal


Candor. Insight. Results.


Disposal - Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

Sample questions to ask:

- Are policies and procedures developed and implemented that address disposal of ePHI, and/or the hardware or electronic media on which it is stored?
- Do the policies and procedures specify the use of a technology, such as, software or a specialized piece of hardware, to make ePHI, and/or the hardware or electronic media, unusable and inaccessible?
- Are the procedures used by personnel authorized to dispose of ePHI, and/or the hardware or electronic media?




Physical Safeguards – Media Re-Use


Candor. Insight. Results.


Media Re-Use - Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

Sample questions to ask:

- Are procedures developed and implemented for removal of ePHI from electronic media before re-use?
- Do the procedures specify situations when all ePHI must be permanently deleted or situations when the electronic media should only be reformatted so that no files are accessible?



Physical Safeguards – Accountability



Candor. Insight. Results.

Accountability - Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

Sample questions to ask:

- Is a process implemented for maintaining a record of the movements of hardware and electronic media containing ePHI?
- Have all types of hardware and electronic media that must be tracked been identified, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards?
- If there are multiple devices of the same type, is there a way to identify individual devices and log or record them separately, such as a serial numbers or other tracking mechanisms?

Physical Safeguards – Data Backup & Storage


Candor. Insight. Results.

Data Backup & Storage - Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Sample questions to ask:

- Is a process implemented for creating a retrievable, exact copy of ePHI, when needed, before movement of equipment?
- Does the process identify situations when creating a retrievable, exact copy of ePHI is required and situations when not required before movement of equipment?
- Does the process identify who is responsible for creating a retrievable, exact copy of ePHI before movement of equipment?



Technical Safeguards

BAKER TILLY
Candor. Insight. Results.

TECHNICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications (R)= Required, (A)=Addressable	
Access Control	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)


Technical Safeguards – Access Control

BAKER TILLY
Candor. Insight. Results.

Unique User Identification - Assign a unique name and/or number for identifying and tracking user identity.

Sample questions to ask:

- Does each workforce member have a unique user identifier?
- What is the current format used for unique user identification?
- Can the unique user identifier be used to track user activity within information systems that contain ePHI?




Technical Safeguards – Emergency Access Procedure

BAKER TILLY
Candor. Insight. Results.


Emergency Access Procedure - Establish procedures for obtaining necessary electronic protected health information during an emergency.

Sample questions to ask:

- Who needs access to the ePHI in the event of an emergency?
- Are there policies and procedures in place to provide appropriate access to ePHI in emergency situations?



Technical Safeguards – Automatic Logoff



Candor. Insight. Results.

Automatic Logoff - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Sample questions to ask:

- Do current information systems have an automatic logoff capability?
- Is the automatic logoff feature activated on all workstations with access to ePHI?


Technical Safeguards – Encryption & Decryption


Candor. Insight. Results.


Encryption & Decryption - Implement a mechanism to encrypt and decrypt electronic protected health information.

Sample questions to ask:

- Which ePHI should be encrypted and decrypted to prevent access by persons or software programs that have not been granted access rights?
- What encryption and decryption mechanisms are reasonable and appropriate to implement to prevent access to ePHI by persons or software programs that have not been granted access rights?



Technical Safeguards – Audit Controls



Candor. Insight. Results.

Audit Controls – Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Sample questions to ask:

- What audit control mechanisms are reasonable and appropriate to implement so as to record and examine activity in information systems that contain or use ePHI?
- What are the audit control capabilities of information systems with ePHI?


Technical Safeguards – Person or Entity Authentication


Candor. Insight. Results.


Person or Entity Authentication – Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Sample questions to ask:

- What types of authentication mechanisms are currently used?
- What level or type of authentication is reasonable and appropriate for each information system with ePHI?
- Are other authentication methods available that may be reasonable and appropriate?



Technical Safeguards – Transmission Security



Candor. Insight. Results.

Integrity Controls - Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Sample questions to ask:

- What security measures are currently used to protect ePHI during transmission?
- Has the risk analysis identified scenarios that may result in modification to ePHI by unauthorized sources during transmission?
- What security measures can be implemented to protect ePHI in transmission from unauthorized access?

Technical Safeguards – Transmission Security



Candor. Insight. Results.

Encryption - Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Sample questions to ask:

- How does the organization transmit ePHI?
- How often does the organization transmit ePHI?
- Based on the risk analysis, is encryption needed to protect ePHI during transmission?
- What methods of encryption will be used to protect the transmission of ePHI?

Administrative Safeguards – Security Awareness



Protection From Malicious Software (Addressable) – Procedures for guarding against, detecting, and reporting malicious software.

Security Reminders (Addressable) - Periodic security updates.

Log-In Monitoring (Addressable) - Procedures for monitoring log-in attempts and reporting discrepancies.

Password Management (Addressable) - Procedures for creating, changing, and safeguarding passwords.

Presenter’s Contact information:
(in order of presentations):

Erika Riethmiller-Bol | Director, Corporate Privacy-Incident Program | Anthem, Inc erika.bol@anthem.com

Chris Duprey, Owner, Caris Consulting, LLC;
chris@carisinnovation.com

Amit Kulkarni, CEO, Secure Healing Inc.
amit@securehealing.com

Daniel Steiner, Senior Manager, Baker Tilly Virchow Krause, LLP
Daniel.Steiner@bakertilly.com
