

HIPAA compliance: Internal controls and security for your healthcare organization

HIPAA: What you should be doing today

Why...

- Safeguarding of PPI (Protected Personal Information) or PII (Personally Identifiable Information) is a requirement of 32 CFR (Code of Federal Regulations), the Privacy Act of 1974
- PHI (Protected Health Information) is a requirement of 45 CFR Section 164.530(c) HIPAA Privacy Rule, which includes PPI.
- Electronic Protected Health Information (ePHI) protection is a requirement of the HIPAA Security Rule (HITECH Act of 2009) and requires a security risk assessment
- The Health Insurance Portability and Accountability Act of 1996.
- HIPAA requires the security of Protected Health Information in any form: paper, photographs, x-rays, verbal communication, fax, phone and electronic transmission.
- It also incorporates, the Privacy Act of 2005, the Anti-Phishing Act of 2005 and the Personal Data Privacy Act of 2005. In essence, anything that identifies a patient is protected by law.

What do I have to protect?

*Source: National Institute of Standards and Technology

1. Names
2. All geographical identifiers smaller than a state, except for the initial 3 digits of a zip code if, according to the current publicly available data from the Bureau of the Census: the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people or, if fewer than 20,000 people, the first three digits are changed to 000.
3. Dates (other than year) directly related to an individual
4. Phone Numbers
5. Fax Numbers
6. Email addresses
7. Social Security numbers
8. Medical record numbers
9. Health Insurance beneficiary numbers

More what do I have to protect?

10. Account Numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers (like laptops, cell phones)
14. Web Uniform Resource Locators (URL's)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger, retinal and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic or code, except the unique code assigned by the investigator to code the data
19. Health Records in any form – Social Media

Who does this apply to & what has to be done?

- Who is governed by these laws?
 - Covered entities (Health Plans, Healthcare Clearinghouses and Providers) who transmit healthcare information electronically. Business Associates who have access to PHI or PPI in any form have the same obligations
- What is required?
 - Policies, Procedures and Processes that are cognizant of the risks of exposure of Protected Health Information or Protected Personal Information (which is a part of PHI) and knowledge by a covered entity of its vulnerabilities, discovered through a risk assessment.

What are your risk areas?

Assess them - start at the beginning

- Do you have a Privacy Officer who understands HIPAA?
- Do you have an anonymous way for employees to report their concerns regarding safeguarding PHI or PPI?
- Do you have a policy of Non-Intimidation/Retaliation
- Do you provide a Notice of Privacy Practices to patients and post where they can readily review?
- Do you have policies & procedures addressing release of patient information?
- Do you have a policy & procedure allowing patient access to their PHI?
- Do you have a process and protocol for responding to subpoenas or court orders for records?
- Do you have a sign-in sheet? Are names visible to other patients?

More risk areas...

- Can receptionist be overheard in the waiting area when talking with a patient or other staff regarding patients?
- Can computer screens be visualized from the check-in window?
- How are paper records stored before scanning into the patient's chart?
- What happens to the paper records afterwards?
- Are physical records stored or left out where cleaning people or other service people have access to them?
- Are documents containing PHI or PPI discarded in the waste basket or disposed of in shred bins. If shred bins, is your shred company bonded – do you have a BAA from them?
- What happens if a patient refuses to share their SS# with you?

And more...

- Are patient records (test results, etc.) hung outside exam rooms if received too late for scanning into the patient chart before their appointment?
- Are people so close at the checkout window they can hear what is going on with other patients?
- Can receptionist or scheduler be overheard from the checkout window as patients are exiting the practice?
- If using a Business Associate Agreement with your vendors, has it been updated since 2013 when major changes took place?
- Have your patient forms been updated to include the changes from 2013 (now includes Business Associates)
- How is the clinical staff notified of the arrival of a patient?
- Do you have a “need to know” policy regarding access to patient info?

And more...

- Where are tablets used by providers, stored after hours?
- Do you allow staff to work from home? If so, are there requirements & policy for maintaining security of PHI/PPI?
- Do you allow physical records to be removed from the office?
- Do you update consents periodically (typically yearly at a minimum) regarding who you can divulge a patient's information to? Do you know the rules for disclosing information to family members, other relatives, close personal friend, partner?
- What kind of information is conveyed by phone from your office? If PHI/PPI – are you verifying who is calling?

And more...

- Do you know where information is going when you fax it?
- Are copier hard drives overwritten at least once per month?
Automatically by security software?
- How are messages sent to patients via email – is it through your secure server to a patient portal requiring patient secure login or via AOL, MSN, etc.
- Do you know when you are required to disclose a breach and who you must notify?
- Do you have policies and procedures that reflect the training staff gets regarding HIPAA and other mandatory trainings?

Data breaches

- OCR (Office of Civil Rights) reports that data breaches are rampant among Business Associates. During a recent poll, 87% indicated they had experienced electronic data security incidents.
- Healthcare providers and payors reported 65% had.
- The original HITECH Act had a limit of 1.5 million as the maximum penalty for all violations of an identical provision.
- That has changed.

Examples of breaches and the resulting fines

- International insurance company with headquarters in Puerto Rico
 - An unencrypted flash drive was stolen from their accounting department containing 2,209 patient accounts with name, address, DOB and SS#.
 - No security or policies
 - Fine was \$2.2 million dollars
- Anthem, Inc.
 - Electronic data breach of 78.8 million patient records
 - \$1.7 million fine
- Premera Blue Cross
 - Electronic data breach of 11 million patient records
 - \$1.5 million fine
- Presence Health
 - Paper OR schedules had disappeared containing 836 names
 - No security or policies
 - Fine was \$475,000
- Excellus Health Plan
 - Electronic data breach of 10 million patient records
 - \$17.3 million

And a few more...

- Advocate Health
 - Data breach of 4 million patients
 - \$5.55 million fine
- NY Presbyterian Hospital/Columbia University
 - Physician tried to deactivate a home computer leaving patient records accessible via internet
 - Fine of \$4.8 million
- Cignet Health
 - Denied 41 patients access to their health records
 - \$4.3 million fine
- University of Mississippi Medical Center
 - Stolen password protected laptop, exposing 10,000 individual's personal information.
 - Failed to notify individual patients and failed to take remedial action
 - \$2.75 million fine
- CVS Pharmacy
 - Threw pill bottles containing patient names, addresses, medications into open dumpster
 - \$2.25 million fine

Cyber security threats and controls to protect information

HIPAA security rule

- In general, the HIPAA Security Rule requires covered entities and business associates to do the following:
 - Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of electronic protected health information (ePHI) that is created, received, maintained or transmitted.
 - Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI.
 - Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required under the Privacy Rule.
 - Ensure compliance with security by its workforce.

Security incidents and data loss

Industry	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
	Total	Small	Large	Unknown	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143	282	136	10	136
Administrative (56)	44	6	3	35	18	6	2	10
Agriculture (11)	4	1	0	3	1	0	0	1
Construction (23)	9	0	4	5	4	0	1	3
Educational (61)	254	16	29	209	29	3	8	18
Entertainment (71)	2,707	18	1	2,688	38	18	1	19
Finance (52)	1,368	29	131	1,208	795	14	94	687
Healthcare (62)	166	21	25	120	115	18	20	77
Information (51)	1,028	18	38	972	194	12	12	170
Management (55)	1	0	1	0	0	0	0	0
Manufacturing (31-33)	171	7	61	103	37	5	11	21
Mining (21)	11	1	7	3	7	0	6	1
Other Services (81)	17	5	3	9	11	5	2	4
Professional (54)	916	24	9	883	53	10	4	39
Public (92)	47,237	6	46,973	258	193	4	122	67
Real Estate (53)	11	3	4	4	5	3	0	2
Retail (44-45)	370	109	23	238	182	101	14	67
Trade (42)	15	3	7	5	4	2	2	0
Transportation (48-49)	31	1	6	24	15	1	3	11
Utilities (22)	24	0	3	21	7	0	0	7
Unknown	9,453	113	1	9,339	270	109	0	161
Total	64,199	521	47,408	16,270	2,260	447	312	1501

Source: 2016 Verizon Data Breach Report

Stats

60%

IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

50%

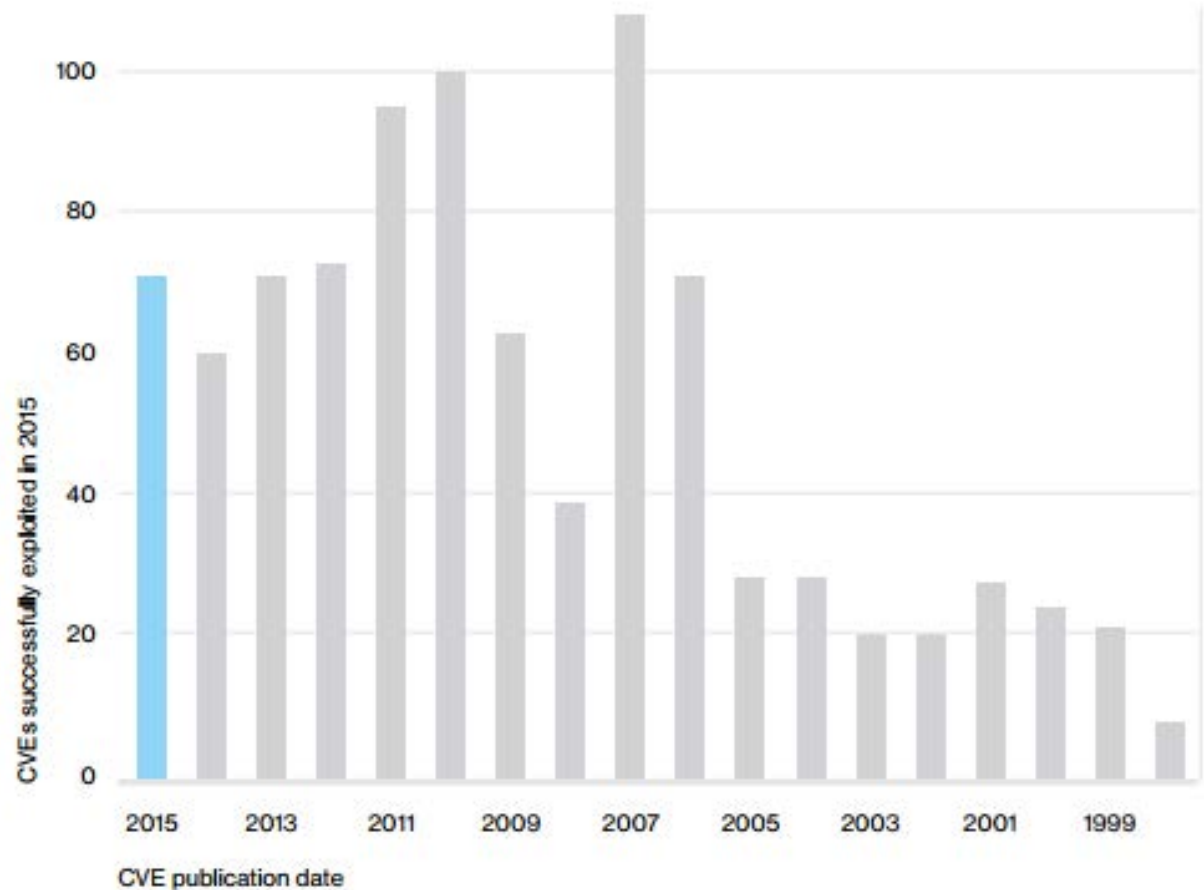
NEARLY 50% OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

23%

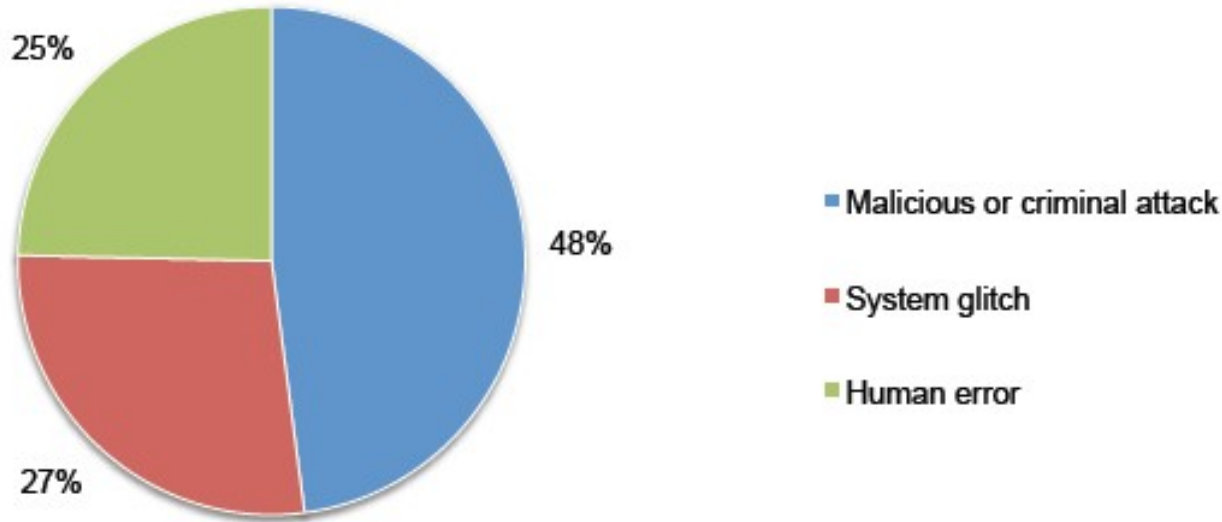
OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

Stats

85% of successful exploit traffic leverage the top 10 vulnerabilities.



The main root causes of a data breach



- The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.
- Negligent insiders are individuals who cause a data breach because of their carelessness

Data breach costs are rising

The difference a year makes

- The average total cost of a data breach increased from \$3.79 to \$4 million (+5.3%)
 - Up 29% since 2013
- The average cost paid for each lost or stolen record containing sensitive and confidential information increased from \$154 to \$158 (+2.6%)
 - Up 15% since 2013

How do cyber criminals get in?

Ransomware	Smishing	Phishing
Vishing	Social Engineering	DDOS
Malware/ Spyware	Keylogging	Skimming

Phishing definition

Definition

The act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do.

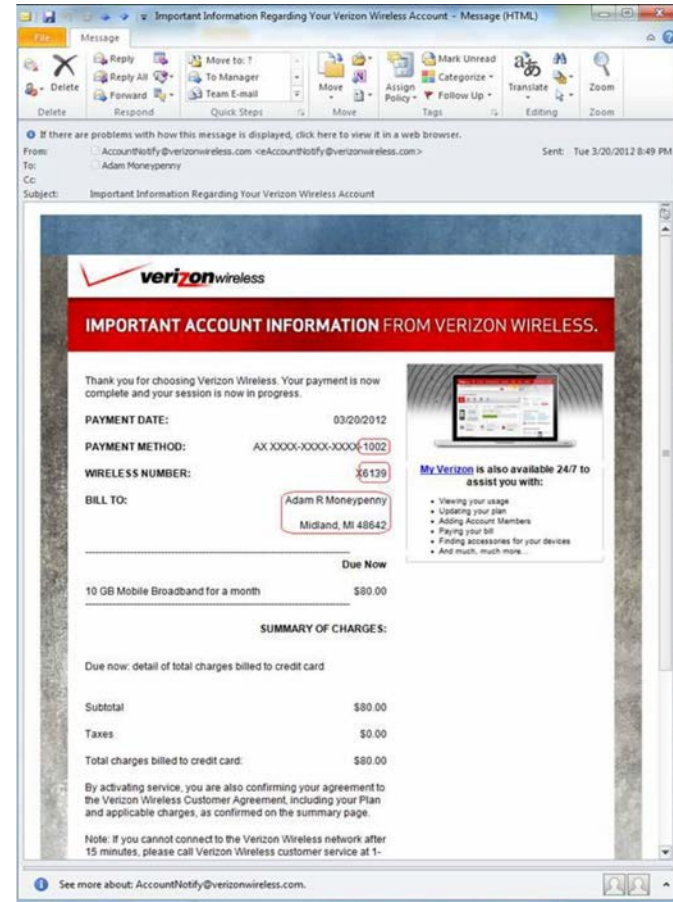
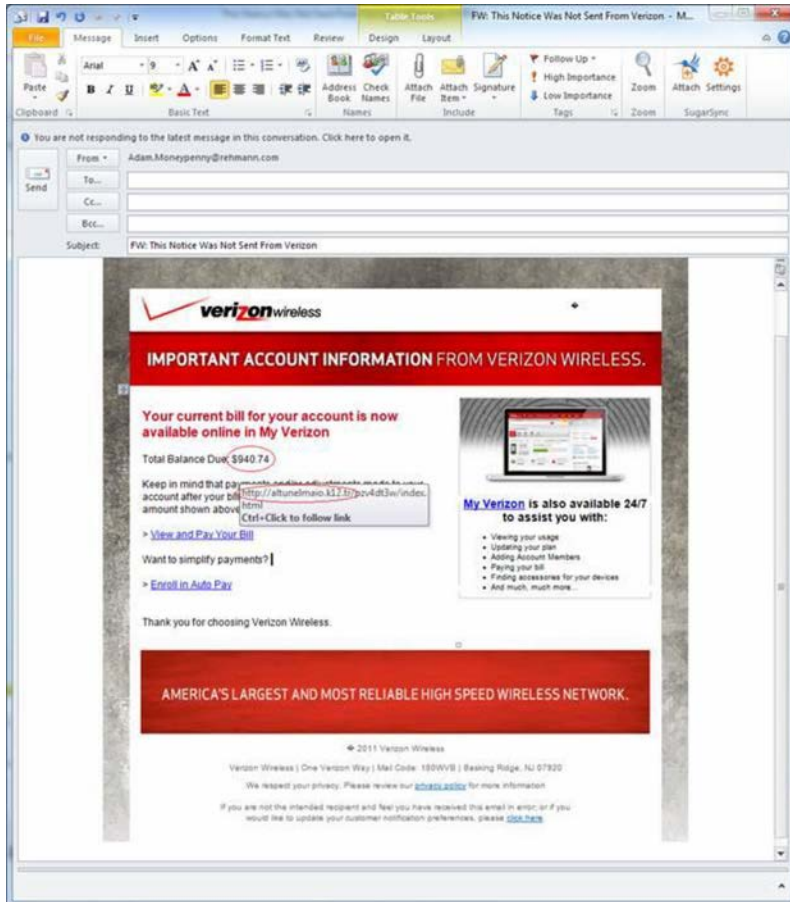
Example

Sending an e-mail to a user falsely claiming to be an established, legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing/Social engineering scams

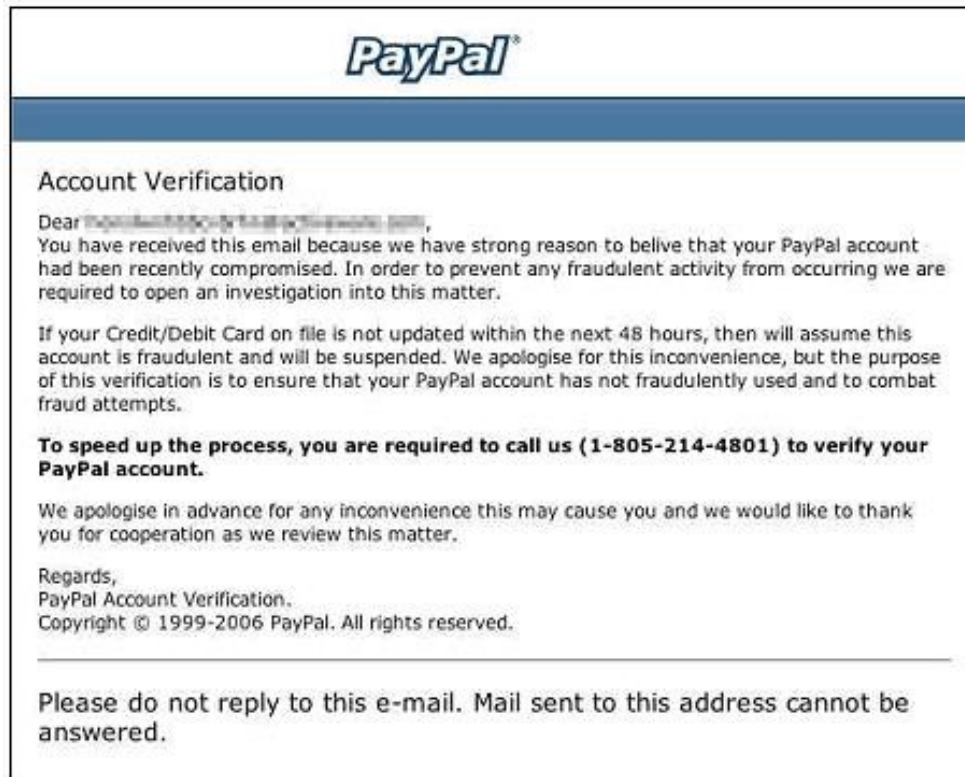
- Email from your internal staff
- Email from your patient
- Message from friend overseas and in trouble
- “Your tax refund is already taken care of”
- Email requesting wire transfer

E-mail social engineering



Vishing

- Phishing with a VoIP twist

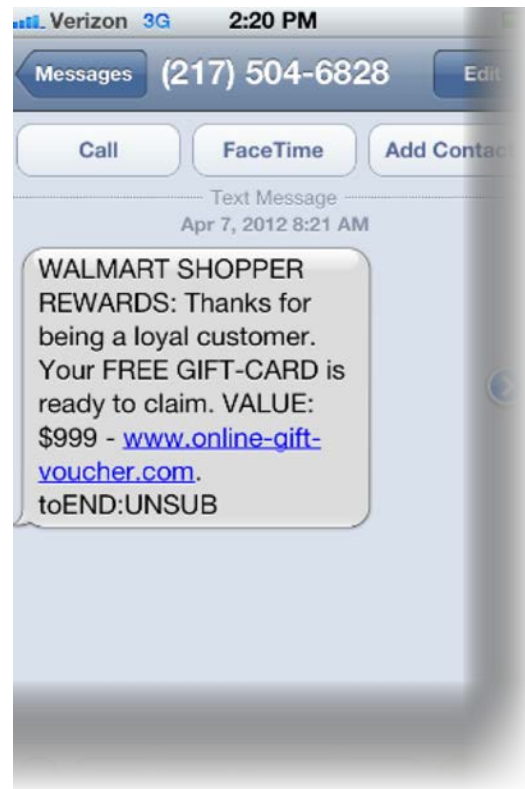


Smishing

- A combination of short message service (SMS or text messaging) and phishing.
- Occurs when scammers pose as trusted companies.
- Send bogus text messages to notify you of account problems.
- They need to verify personal information and provide Web sites or telephone numbers for you to do so.

Smishing

- It might come from familiar source



Ransomware

- Your data taken “hostage”
- Ransom email
- Today \$300
- Tomorrow more
- If you don't pay, they destroy your data

DDoS

- A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic.

Malware/Spyware

- Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, trojan horses, and spyware.

Keylogging

- The use of a computer program to record every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.

2015 most common passwords

1. **123456** (Unchanged)
2. **password** (Unchanged)
3. **12345678** (Up 1)
4. **qwerty** (Up 1)
5. **12345** (Down 2)
6. **123456789** (Unchanged)
7. **football** (Up 3)
8. **1234** (Down 1)
9. **1234567** (Up 2)
10. **baseball** (Down 2)

Employees are the weakest link

- Negligent insiders are the top cause of data breaches
- Clicking on links in emails
- Sending work email to personal accounts
- Using company data on insecure lines
- Not following corporate policies
- Not securing mobile devices

Vulnerability: Weak IT security

- Poor access controls
- Poor patch management
- Improper device configuration
- Lack of security audits
- Weak enforcement of remote login policies

Controls combat incidents

CSC	DESCRIPTION	PERCENTAGE	CATEGORY
13-7	2FA	24%	Visibility/Attribution
6-1	Patching web services	24%	Quick Win
11-5	Verify need for Internet-facing devices	7%	Visibility/Attribution
13-6	Proxy outbound traffic	7%	Visibility/Attribution
6-4	Web application testing	7%	Visibility/Attribution
16-9	User lockout after multiple failed attempts	5%	Quick Win
17-13	Block known file transfer sites	5%	Advanced
5-5	Mail attachment filtering	5%	Quick Win
11-1	Limiting ports and services	2%	Quick Win
13-10	Segregation of networks	2%	Configuration/Hygiene
16-8	Password complexity	2%	Visibility/Attribution
3-3	Restrict ability to download software	2%	Quick Win
5-1	Anti-virus	2%	Quick Win
6-8	Vet security process of vendor	2%	Configuration/Hygiene

40%
 OF CONTROLS
 DETERMINED TO BE
 MOST EFFECTIVE FALL
 INTO THE *QUICK WIN*
 CATEGORY.

How we apply the security rule

- Administrative Safeguards
 - Policies and procedures are REQUIRED and must be followed by employees to maintain security (i.e. disaster, internet and e-mail use)
- Technical Safeguards
 - Assignment of different levels of access
 - Screen savers
 - Devices to scan ID badges
 - Audit trails
- Physical Safeguards
 - Lock doors
 - Monitor visitors
 - Secure unattended computers



How we apply the security rule

- Policies and Procedures
- Internet Use
 - Access only trusted, approved sites
 - Don't download programs to your workstation
- E-Mail
 - Keep e-mail content professional
 - Use work e-mail for work purposes only
 - Don't open e-mails or attachments if you are suspicious of or don't know the sender
 - Don't forward jokes
 - Follow policy for sending secure e-mails

How we apply the security rule

- How do we control ePHI access?
 - User names and passwords
 - Biometrics
 - Screen savers
 - Automatic logoff



Access to ePHI

- Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in the HIPAA Security Rule.



Access to ePHI

- Assign a unique name and/or number for identifying and tracking user identity. It enables an entity to hold users accountable for functions performed on information systems with ePHI when logged into those systems.



Access to ePHI

- The Security Rule requires organizations to implement procedures regarding access controls, which include the creation and use of passwords, to verify that a person or entity seeking access to ePHI is the one claimed.
- The use of a strong password to protect access to ePHI is an appropriate and expected risk management strategy.


Access to ePHI

What Makes a Strong Password?

- Use at least 8 characters.
- Use letters, numbers, upper and lower case letters, and special characters
- Use a “pass-phrase” such as MbcFi2yo (My brown cat Fluffy is two years old)
- Do not use passwords that others may be able to guess:
 - Spouse’s Name, Pet or Child’s Name
 - Significant Dates
 - Favorite sports teams



What can I do to help protect our computer systems and equipment?

- Workstation use
 - Restrict viewing access to others
 - Follow appropriate log-on and log-off procedures
 - Lock your workstation, press Ctrl-Alt-Del or Windows key  + “L”
 - Use automatic screen savers that lock your computer when not in use
- Do not add your own software and do not change or delete software that is the property of the organization
- Know and follow organizational policies
- If devices are lost, stolen or compromised, notify your supervisor immediately!
- Do not store PHI on mobile devices unless you are authorized to do so and appropriate security safeguards have been implemented by your organization



Let's talk cell phones (PDA's)

- Are all business cell phones biometric or password protected?
- Are personal cell phones used for business? What is the policy?
- Where are business cell phones stored when not in use?
- Is PII or PHI routinely downloaded to PDA's (rounds, emails concerning patients, appointment schedules)?
- Is that information encrypted?
- Is there tracking software on each business phone?
- Is remote wipe utilized?

E-mail security

- Appropriate use of e-mail can prevent the accidental disclosure of ePHI. Some tips or best practices include:
 - Use email in accordance with policies and procedures defined by the organization.
 - Use e-mail for business purposes and do not use e-mail in a way that is disruptive, offensive, or harmful.
 - Verify email address before sending.
 - Include a confidentiality disclaimer statement.
 - Don't open e-mail containing attachments when you don't know the sender.

Audit Controls

- The Security Rule requires organizations to implement hardware, software, and/or procedural mechanisms that record and examine activity in electronic information systems that contain or use ePHI.
- Organizations should define the reasons for establishing audit trail mechanisms and procedures for its electronic information systems that contain ePHI.
- Reasons may include, but are not limited to,
 - Policy enforcement
 - Compliance with the Security Rule
 - Mitigating risk of security incidents
 - Monitoring workforce member activities and actions

In the end...



Q&A Session



Kathy Jo Uecker
CMPE, EFPM, NCP, CPC, COC, CHSPA,
CHSA
AHIMA Trainer for ICD10CM/PCS
Healthcare Consultant
NetSource One, Inc.
Kathyjo.uecker@nsoit.com
www.nsoit.com
(989)797-1092 | fax: (269)798-5920
(269)420-9404 cell

