MedPro Group

a Berkshire Hathaway company

PEACE OF MIND | EXPERTISE | CHOICE | THE MEDPRO GROUP DIFFERENCE

HIPAA Privacy and Security Essentials

Today's program

Joyce Bruce, RN, MSN, JD, CPHRM
AVP, Patient Safety & Risk Solutions, MedPro Group
(Joyce.Bruce@medpro.com)

Joyce provides comprehensive services to healthcare systems, hospitals, and clinics. She has more than 20 years of experience in the healthcare industry working in clinical practice, hospital administration, law, and consulting.

Joyce's extensive clinical leadership includes experience as director of nursing in tertiary and pediatric facilities. In these roles, she led the development of quality programs, delivery of care models, and clinical care paths, including the creation of data collection systems. In addition to her healthcare background and expertise, Joyce's legal experience includes insurance defense, criminal defense, and healthcare law.

In previous positions, Joyce also provided risk management consulting services, including program development, educational services, risk reduction, accreditation surveys, and regulatory compliance (including EMTALA and HIPAA). She also participated in the development of best policies for physician groups and hospitals.

Joyce is a graduate of Indiana University with a bachelor of science degree in nursing and a master of science degree in nursing administration. Joyce earned her juris doctorate from Indiana University-Indianapolis. She is a member of the Indiana Bar, Ohio Bar, American Society for Healthcare Risk Management, the American Association of Nurse Attorneys, and the Ohio Society for Healthcare Risk Management. She also is a certified professional in healthcare risk management (CPHRM).

Designation of continuing education credit

MedPro Group is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

MedPro Group designates this enduring activity for a maximum of 1.0 AMA PRA Category 1 Credits™. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

MedPro Group is designated as an Approved PACE Program Provider by the Academy of General Dentistry. The formal continuing dental education programs of this program provider are accepted by AGD for Fellowship/Mastership and membership maintenance credit. Approval does not imply acceptance by a state or provincial board of dentistry or AGD endorsement. The current term of approval extends from October 1, 2018 to September 30, 2022. Provider ID# (218784)

MedPro Group designates this continuing dental education activity, as meeting the criteria for up to 1 hour of continuing education credit. Doctors should claim only those hours actually spent in the activity.

Disclosure

MedPro Group receives no commercial support from pharmaceutical companies, biomedical device manufacturers, or any commercial interest.

It is the policy of MedPro Group to require that all parties in a position to influence the content of this activity disclose the existence of any relevant financial relationship with any commercial interest.

When there are relevant financial relationships, the individual(s) will be listed by name, along with the name of the commercial interest with which the person has a relationship and the nature of the relationship.

Today’s faculty as well as CE planners, content developers, reviewers, editors, and Patient Safety & Risk Solutions staff at MedPro Group have reported that they have no relevant financial relationships with any commercial interests.

Objectives

By the end of this program, participants should be able to:

- Review key provisions of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules
- Discuss common vulnerabilities in healthcare practices and organizations that result in HIPAA breaches
- Identify best practices that might mitigate the risk of breaches
- Understand how to respond to incidents and breaches
- Discuss HIPAA considerations for electronic communications
- Discuss fines and penalties for HIPAA noncompliance
- Review best practices to reduce the incidence and impact of cyberattacks and ransomware

Definitions and acronyms

Breach	Impermissible use or disclosure of PHI that compromises the security or privacy of the PHI
Business associate (BA)	Person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE
Business associate agreement (BAA)	Legal contract that describes how the BA adheres to HIPAA along with the responsibilities and risks it assumes
Covered entity (CE)	Healthcare provider, health plan, or healthcare clearinghouse that electronically transmits any health information
Protected health information (PHI)	Information the CE creates or receives that identifies the patient, including demographic information (e.g., addresses, phone numbers, etc.). PHI relates to a patient’s past, present, or future physical or mental health or condition. e-PHI: Electronic PHI

Key provisions

HIPAA provides a patient the right to his/her PHI including:

- A notice on how the practice or organization uses PHI
- An individual's right to a copy of his/her health records
- A right to request restrictions on release of his/her PHI
- A right to request changes (amendments) to his/her health records
- A right to request an accounting of disclosures of an individual's PHI
- Restrictions on the disclosure or use of PHI without an individual's authorization
- A right to receive confidential communications
- A right to file a complaint for privacy rights violations

HIPAA privacy requirements for covered entities

- Identify a HIPAA Privacy Officer
- Ensure that all staff, volunteers, students, etc., are trained and annually updated
- Identify all BAs and maintain BAAs with them
- Develop and implement HIPAA privacy policies (minimally):
  - What is defined as your designated record set
  - Posting of Notice of Privacy Practices
  - Minimum necessary standard
  - Release of records/disclosure of PHI
  - Requests for restrictions
  - Requests for amendments
  - Requests for an accounting of disclosure
  - The use and disclosure of an individual’s PHI

Basic rules on releasing protected health information

- Patients' information can be released without authorization if the purpose is for treatment, payment, or healthcare operations.
- Disclosure of patients' PHI for anything other than treatment, payment, or healthcare operations requires completion of an authorization.
- Certain exceptions exist for public health monitoring activities (e.g., disease reporting), government oversight, and some law enforcement investigations. Staff should always consult with the HIPAA Privacy Officer to ensure proper release.

Responding to a patient’s request for health records

- Must provide health records no later than 30 days from the request unless a state law requires sooner
- Only three costs may be charged to the patient:
  - Reasonable cost of labor for creating and delivering the health records in the form and format requested
  - Costs of supplies for creating the paper copy (such as paper or toner) or electronic copy (such as a USB drive)
  - Actual cost of postage if the patient has requested for records to be mailed
  - Costs associated for reviewing the request, searching for and retrieving health records, or preparing the health records for copying cannot be charged
- A patient’s health records should never be withheld for outstanding balances

What is the minimum necessary standard?

Whenever patients' PHI is used or disclosed, whether to another CE or BA, only the information necessary to accomplish the intended purpose should be disclosed.

Example: The practice uses a collection agency that has requested billing information on several patients. The practice sends the billing information, but also includes patients' diagnostic information. The collection agency does not need the diagnostic information to perform its tasks; thus, the practice violated the minimum necessary standard.

Common privacy rule vulnerabilities that result in breaches

Failure to . . . results in breaches

- Orient and train staff; provide updates and ongoing education
- Identify a HIPAA Privacy Officer
- Have policies and procedures in place
- Adhere to the minimum necessary standard for accessing and releasing PHI
- Identify all BAs
- Obtain BAAs
- Have an incident and breach response process in place

Best privacy practices to mitigate the risk of breach

- Ensure provider and staff orientation and ongoing education
- Implement organizational policies and procedures (minimally):
  - Notice of Privacy Practices
  - Release of records
  - Requests for restrictions
  - Requests for amendments
  - Accounting of disclosures
  - Corrective action
  - Breach responses
  - Responding to complaints
- Identify a Privacy and Security Officer
- Comply with minimum necessary standard in accessing PHI and release of information

Frequently asked questions

Q: Can I provide copies of records to other providers without a patient's authorization?

A: Yes, if the request is for treatment purposes.

Q: If a patient requests records, do I need to provide copies of other providers' records?

A: Yes, any record that a provider uses for treatment decisions, regardless of whether generated by him/her, is part of the designated record set. If a provider references outside notes or labs from another provider, then they become part of the designated record set.

Q: The patient asks for his/her original record. Can I provide the original?

A: You should never release the original record because it's the property of the healthcare organization. HIPAA stipulates that patients may receive a copy. However, you can offer to allow the patient to inspect the original record onsite with a staff member present.

Q: The patient has requested that we do not provide information to his/her insurance company. Must we honor that request?

A: Yes, you are required to comply with the request as long as the patient pays for the services out of pocket.

HIPAA Privacy and Security Rules

Key provisions of the HIPAA Security Rule

The HIPAA Security Rule protects information covered by the Privacy Rule, which is all individually identifiable health information a CE creates, receives, maintains, or transmits in electronic form (e-PHI). The Security Rule does not apply to PHI transmitted orally or in writing.

The HIPAA Security Rule requires CEs to maintain and protect e-PHI through reasonable and appropriate:

- Administrative safeguards
- Technical safeguards
- Physical safeguards

HIPAA security requirements for covered entities

Ensure the confidentiality, integrity, and availability of all e-PHI that the CEs create, receive, maintain, or transmit

Identify and protect against reasonably anticipated threats to the security or integrity of the information

Protect against reasonably anticipated, impermissible uses or disclosures

Ensure compliance by their workforce

Perform a risk analysis as part of their security management processes and update regularly

Risk analysis components

A risk analysis process should minimally include:

- Evaluation and likelihood of the impact of potential risks to e-PHI
- Risks identified in the risk analysis
- Appropriate security measures taken to address the identified risks
- Documentation of the security measures taken and the rationale for adopting those security measures

Maintain continuous, reasonable, and appropriate security protections

Administrative safeguards

- Security management process
  - Includes completion of a risk analysis, identifying vulnerabilities and implementation of security measures to address
- Designation of a HIPAA Security Officer
- Information access management
  - Policies and procedures for authorizing access to e-PHI based on the user or recipient's role (role-based access)
- Workforce training and management
  - All workforce members must be trained on its security policies and procedures
  - Must have and apply appropriate sanctions against workforce members who violate its policies and procedures
- Evaluation
  - Periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule

Technical safeguards

- Facility access and control
  - Must have physical limits in accessing its facilities while ensuring that authorized access is allowed
- Workstation and device security
  - Must have policies and procedures to specify proper use of and access to workstations and electronic media (laptops, thumb drives, email, websites)

Physical safeguards

- Access controls
  - Policies and procedures that allow only authorized persons to access e-PHI
- Audit controls
  - Must implement hardware, software, or other procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI
- Integrity controls
  - Policies and procedures and electronic measures to ensure that e-PHI is properly destroyed
- Transmission security
  - Implement technical security measures that guard against unauthorized access to e-PHI being transmitted over an electronic network

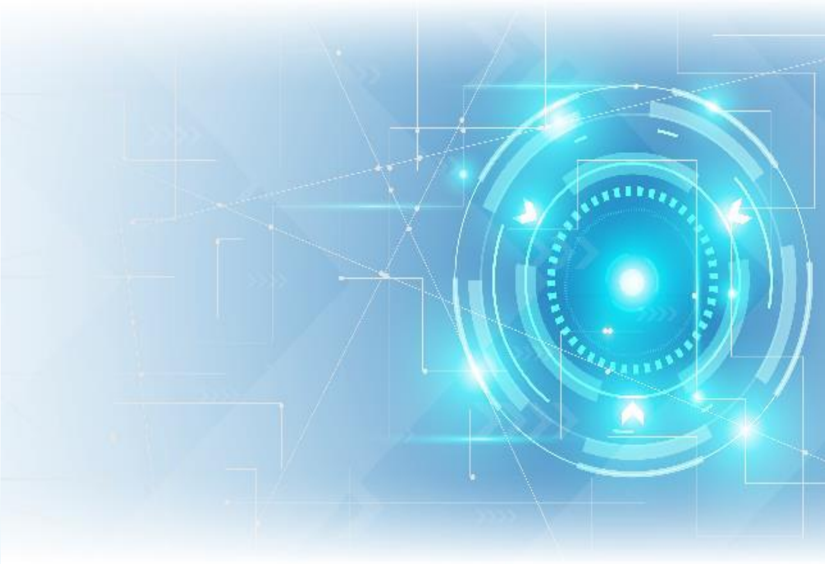
Common security vulnerabilities that result in breaches

Failure to . . . results in breaches

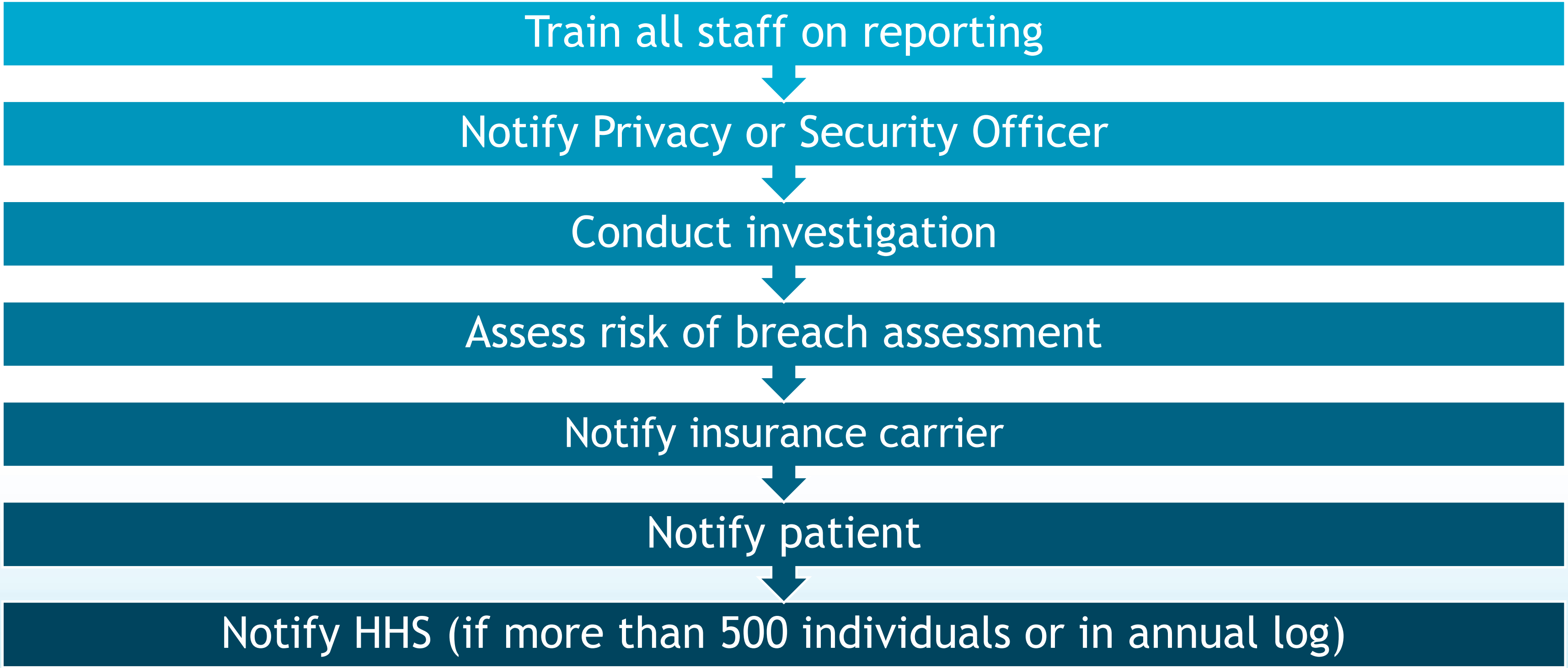
- Conduct a security analysis and address vulnerabilities
- Use encryption and secure email
- Comply with the minimum necessary standard and limitations on authorizations
- Identify BAs and obtain BAAs
- Conduct staff training
- Update programs and patches

Best practices to mitigate security breaches

- Conduct staff training on identifying and reporting potential incidents and breaches, use, and risks
- Place encryption on all electronic devices, including portable devices and thumb drives
- Implement schedules and assign accountability for program updates and patches
- Use medical equipment and the “Internet of things” (IoT) such as cardiac pacemakers, drug administration devices, monitoring devices, infusion pumps, defibrillators, glucometers, and blood pressure measurement devices
- Put appropriate physical safeguards in place



Responding to security incidents and breaches



Train all staff on reporting

Notify Privacy or Security Officer

Conduct investigation

Assess risk of breach assessment

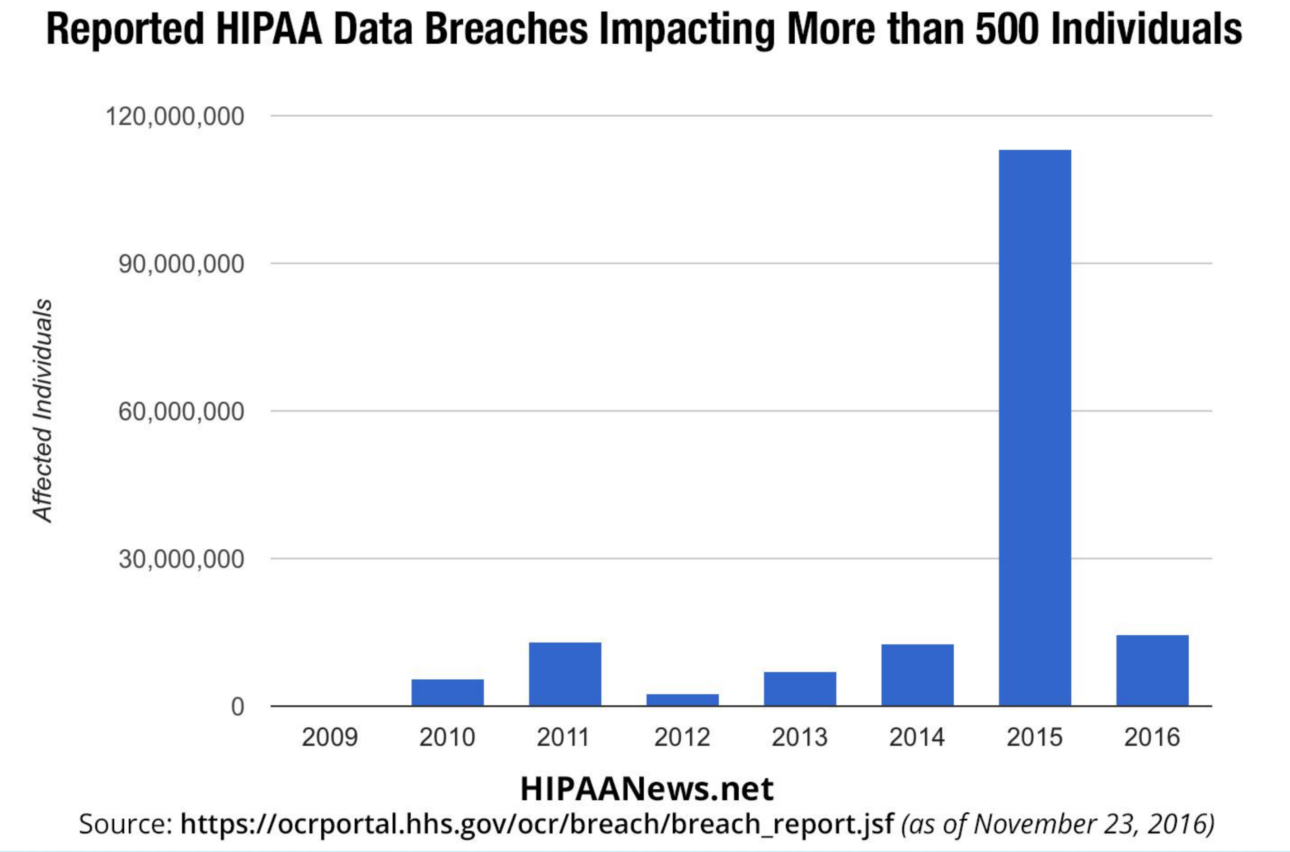
Notify insurance carrier

Notify patient

Notify HHS (if more than 500 individuals or in annual log)

HHS: U.S. Department of Health and Human Services

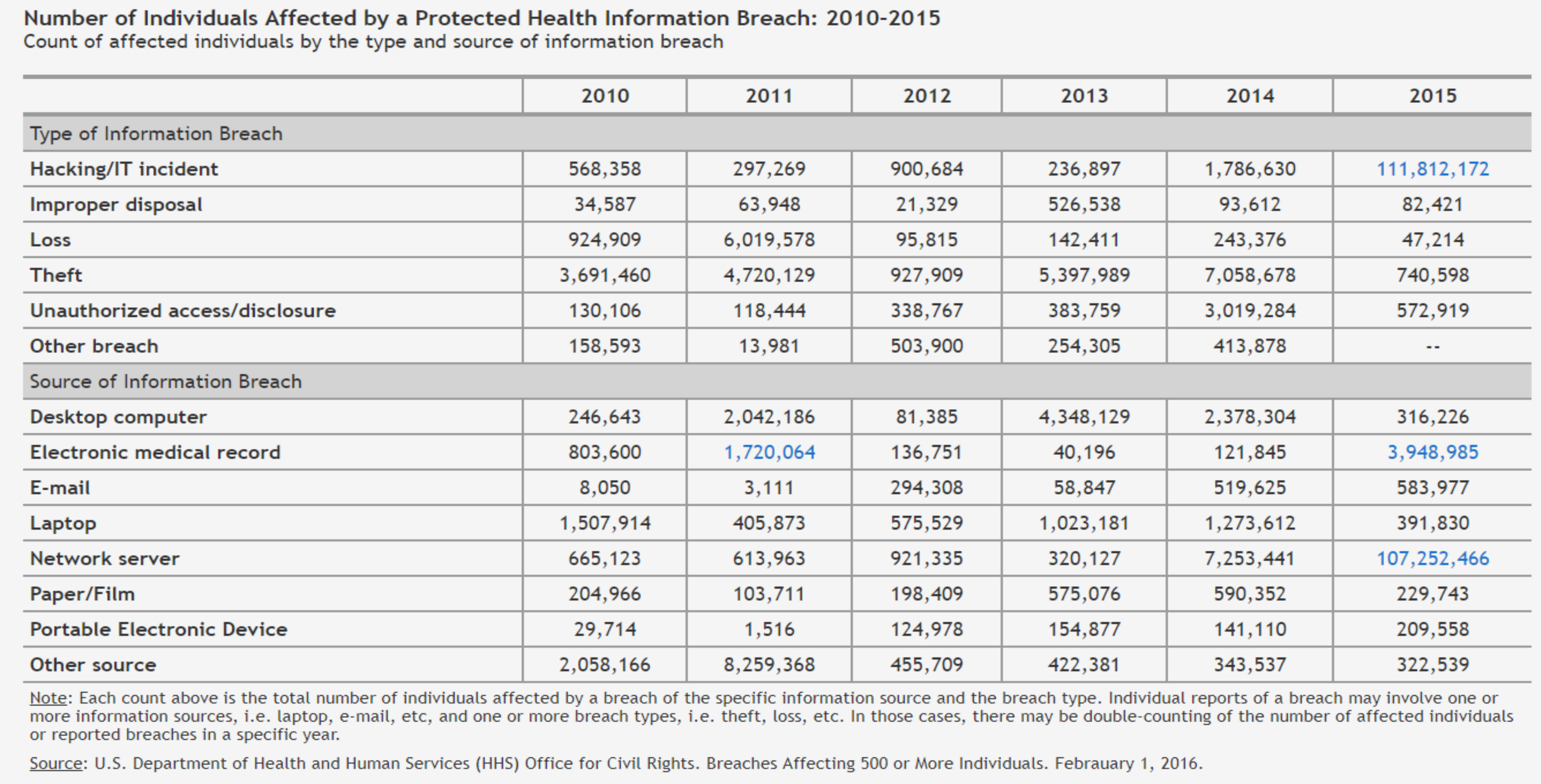
Data breaches



Source: **https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf** *(as of November 23, 2016)*

Source: U.S. Department of Health and Human Services Office for Civil Rights. (2018). Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Types and sources of breaches



Number of Individuals Affected by a Protected Health Information Breach: 2010-2015
Count of affected individuals by the type and source of information breach

	2010	2011	2012	2013	2014	2015
Type of Information Breach						
Hacking/IT incident	568,358	297,269	900,684	236,897	1,786,630	111,812,172
Improper disposal	34,587	63,948	21,329	526,538	93,612	82,421
Loss	924,909	6,019,578	95,815	142,411	243,376	47,214
Theft	3,691,460	4,720,129	927,909	5,397,989	7,058,678	740,598
Unauthorized access/disclosure	130,106	118,444	338,767	383,759	3,019,284	572,919
Other breach	158,593	13,981	503,900	254,305	413,878	--
Source of Information Breach						
Desktop computer	246,643	2,042,186	81,385	4,348,129	2,378,304	316,226
Electronic medical record	803,600	1,720,064	136,751	40,196	121,845	3,948,985
E-mail	8,050	3,111	294,308	58,847	519,625	583,977
Laptop	1,507,914	405,873	575,529	1,023,181	1,273,612	391,830
Network server	665,123	613,963	921,335	320,127	7,253,441	107,252,466
Paper/Film	204,966	103,711	198,409	575,076	590,352	229,743
Portable Electronic Device	29,714	1,516	124,978	154,877	141,110	209,558
Other source	2,058,166	8,259,368	455,709	422,381	343,537	322,539

Note: Each count above is the total number of individuals affected by a breach of the specific information source and the breach type. Individual reports of a breach may involve one or more information sources, i.e. laptop, e-mail, etc, and one or more breach types, i.e. theft, loss, etc. In those cases, there may be double-counting of the number of affected individuals or reported breaches in a specific year.

Source: U.S. Department of Health and Human Services (HHS) Office for Civil Rights. Breaches Affecting 500 or More Individuals. Febrauary 1, 2016.

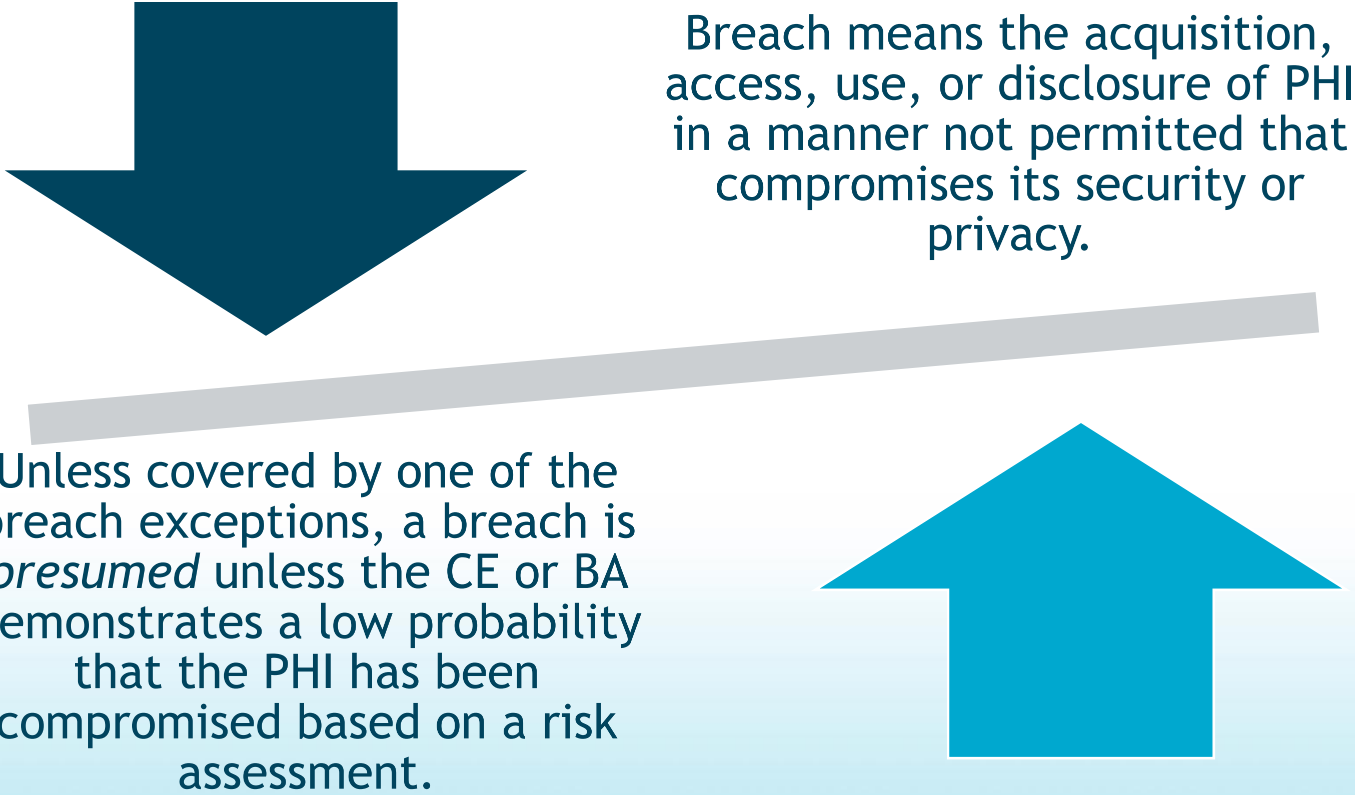
Source: U.S. Department of Health and Human Services Office for Civil Rights. (2016, February 1). Breaches affecting 500 or more individuals. Washington, DC: HHS.

Breach notification examples

- Looking at a neighbor’s health records out of curiosity
- Mailing billing information to the wrong patient
- Losing an unencrypted thumb drive
- Talking to a family member about a patient
- Losing a phone with patient images on it
- Lost or stolen computer that contains PHI

A supervisor or the Privacy Officer should be immediately notified if an incident or breach is suspected or believed to have occurred.

Responding to incidents and breaches



Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted that compromises its security or privacy.

Unless covered by one of the breach exceptions, a breach is *presumed* unless the CE or BA demonstrates a low probability that the PHI has been compromised based on a risk assessment.

Risk of breach assessment

Must minimally include at least the following factors:

- Nature and extent of the PHI involved
- The unauthorized person(s) who used the PHI or to whom the disclosure was made
- Whether the PHI was actually acquired or viewed
- The extent to which the risk has been mitigated

Notification

Notification of fewer than 500 must be logged and reported 60 days after the calendar year they are discovered.

Breaches of more than 500 must be reported immediately to HHS and the local media outlet.

No change in information required in breach notification letters.

No change in timeframe for reporting 60 days from date of discovery or when with reasonable diligence should have been discovered.

HHS: U.S. Department of Health and Human Services

Special considerations for electronic communications

Texting

- Orders are prohibited
- Messages should be on encrypted text platforms

Email

- Secure encrypted systems

Telemedicine

- Account for privacy and security considerations

Fines and penalties

Civil monetary penalties

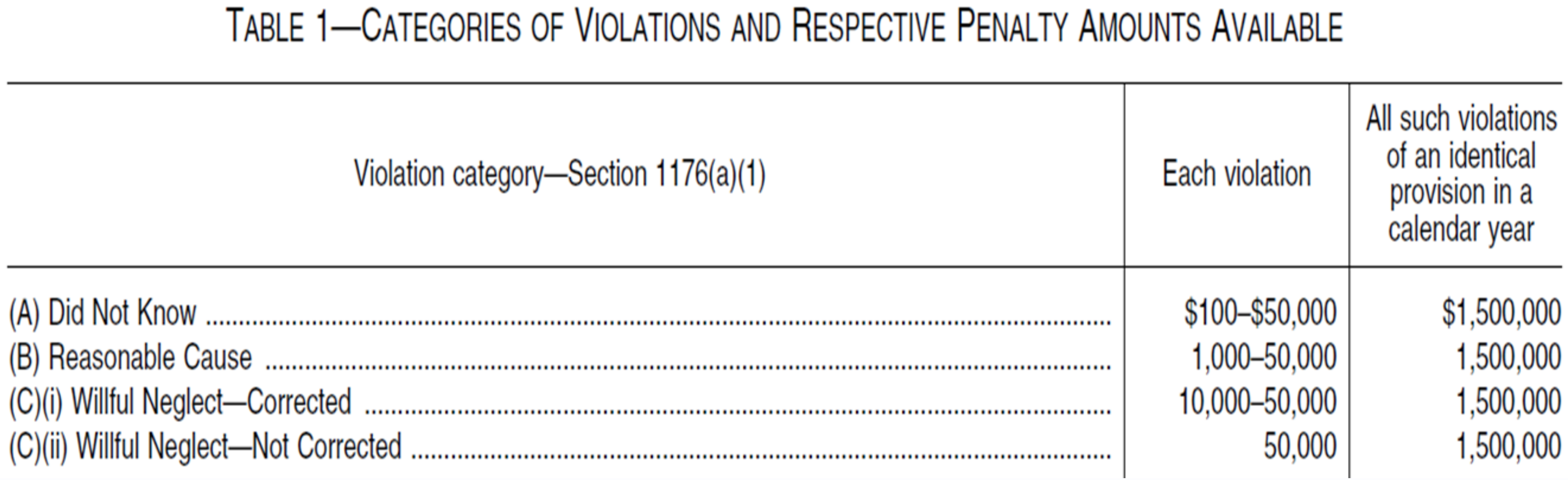


TABLE 1—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	$100–$50,000	$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000

- Failure to comply with policies and procedures may result in corrective action
- CEs (including individual employees) and BAs are subject to civil monetary penalties (fines) and criminal penalties

Criminal penalties

- Prohibited conduct
  - Knowingly obtaining or disclosing PHI without authorization
  - If done under false pretenses
  - If done with intent to sell, transfer, or use the information for commercial advantages, personal gain, or malicious harm
- Penalty
  - Up to $50,000 fine and 1 year in prison
  - Up to $100,000 fine and 5 years in prison

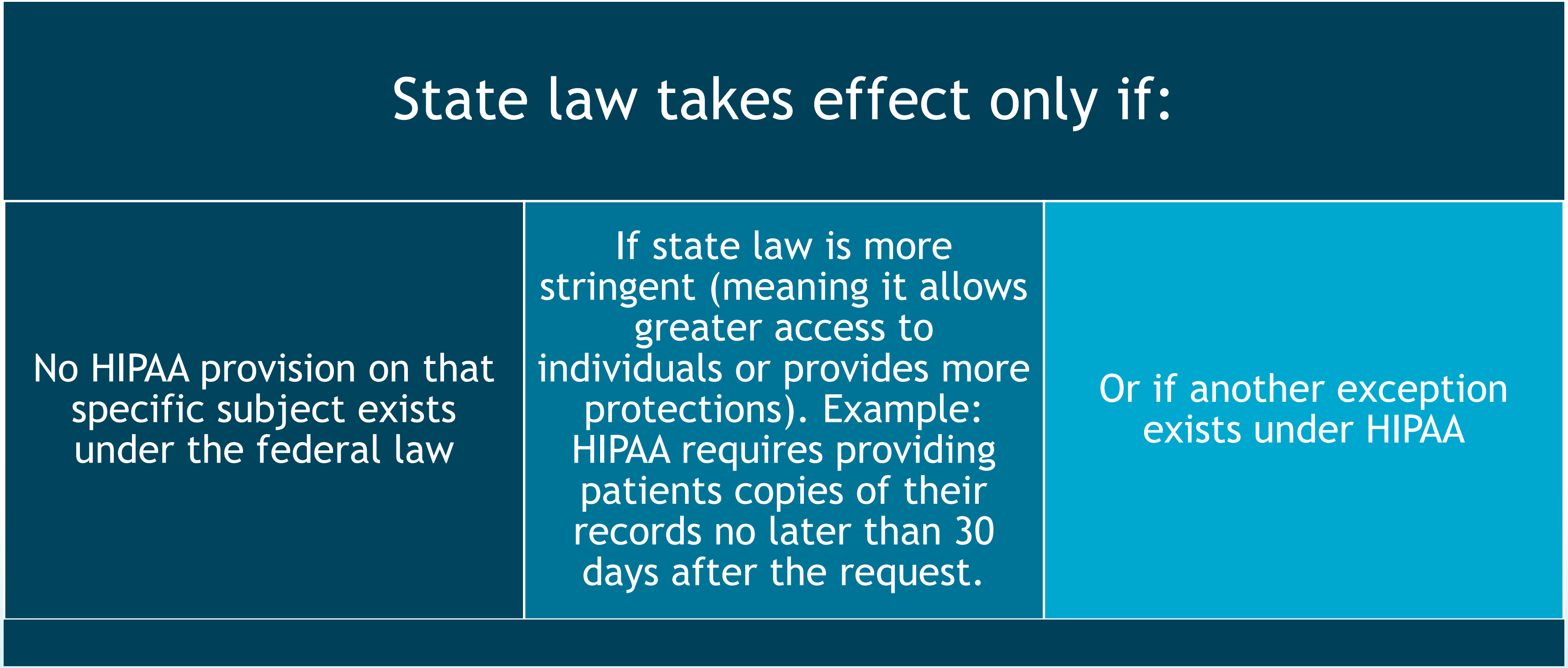
Source: 42 U.S.C. § 1320d-5(d)

State Attorneys General offices

Health Information Technology for Clinical and Economic Health (HITECH) Act provides State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules.

The HITECH Act permits State Attorneys General to obtain damages on behalf of state residents or to enjoin further violations of the HIPAA Privacy and Security Rules.

State HIPAA laws



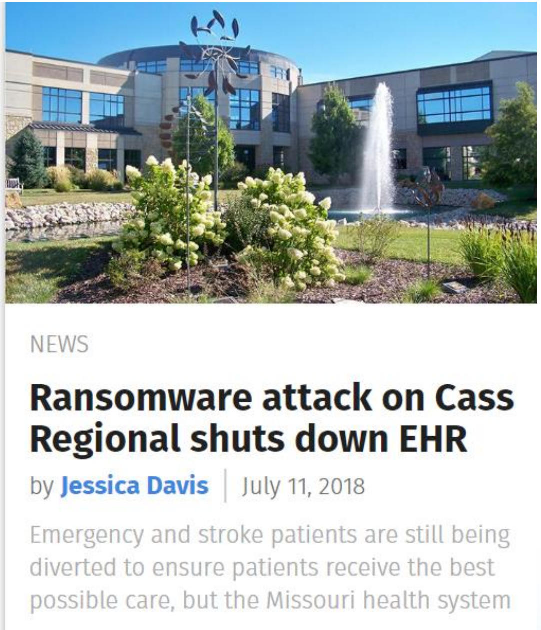
State law takes effect only if:

No HIPAA provision on that specific subject exists under the federal law

If state law is more stringent (meaning it allows greater access to individuals or provides more protections). Example: HIPAA requires providing patients copies of their records no later than 30 days after the request.

Or if another exception exists under HIPAA

Cyberattacks and ransomware

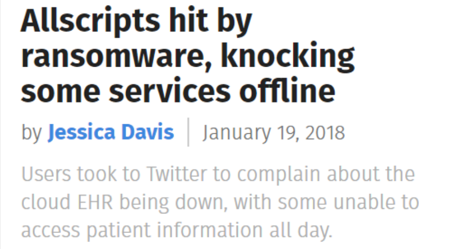


NEWS

Ransomware attack on Cass Regional shuts down EHR

by Jessica Davis | July 11, 2018

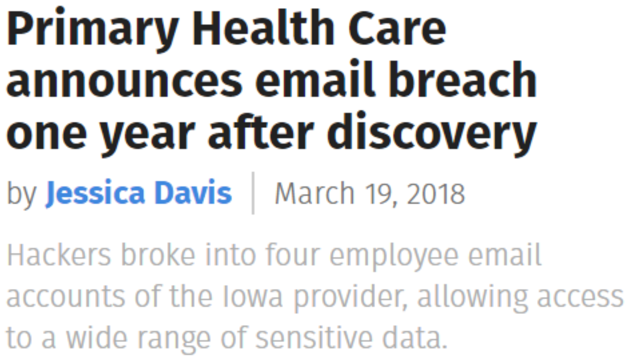
Emergency and stroke patients are still being diverted to ensure patients receive the best possible care, but the Missouri health system



Allscripts hit by ransomware, knocking some services offline

by Jessica Davis | January 19, 2018

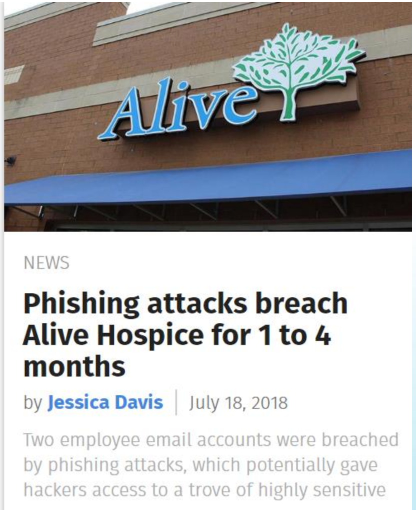
Users took to Twitter to complain about the cloud EHR being down, with some unable to access patient information all day.



Primary Health Care announces email breach one year after discovery

by Jessica Davis | March 19, 2018

Hackers broke into four employee email accounts of the Iowa provider, allowing access to a wide range of sensitive data.

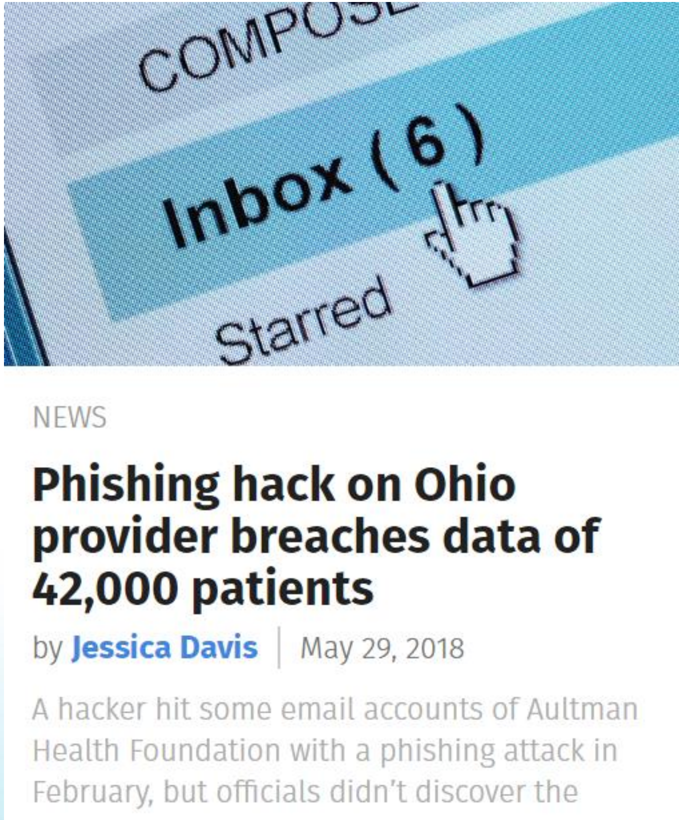


NEWS

Phishing attacks breach Alive Hospice for 1 to 4 months

by Jessica Davis | July 18, 2018

Two employee email accounts were breached by phishing attacks, which potentially gave hackers access to a trove of highly sensitive



NEWS

Phishing hack on Ohio provider breaches data of 42,000 patients

by Jessica Davis | May 29, 2018

A hacker hit some email accounts of Aultman Health Foundation with a phishing attack in February, but officials didn't discover the

Frequently seen vulnerabilities in healthcare

- Multiple and niche software vendors
- Fragmented interoperability; variation in practices, policies, and technologies
- Failure to provide resources for updates, upgrades, enhancements, and education
- Limited ability and pressure on downtime to make electronic record changes
- Medical devices and vendor systems
- Lack of education and training

Impact and potential outcomes of cyber attacks

Patient safety

- Inaccessible patient history and information limiting the ability to treat

Financial impact

- Lost billing records and clinical records to support billing

Incident investigation

- Forensic use and resources

Breach determination and notification

- Risk of breach assessment notification

State and federal investigations and fines

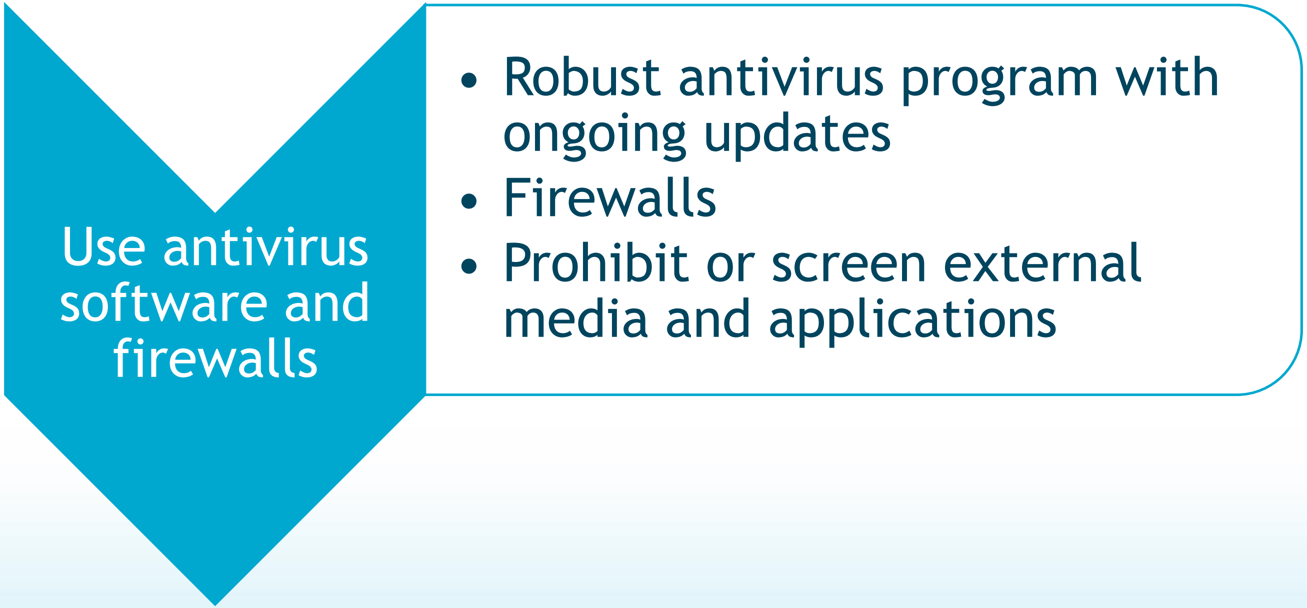
Credibility and reputation

Strategies/best practices to avoid and mitigate cyber risk

<u>Passwords</u>

- Must be strong – minimum 8 characters with at least one number/letter/cap/ special character
- Need to change on a schedule basis
- Use multifactor authentication (fingerprint, fob, etc.)

Strategies/best practices to avoid and mitigate cyber risk



Use antivirus software and firewalls

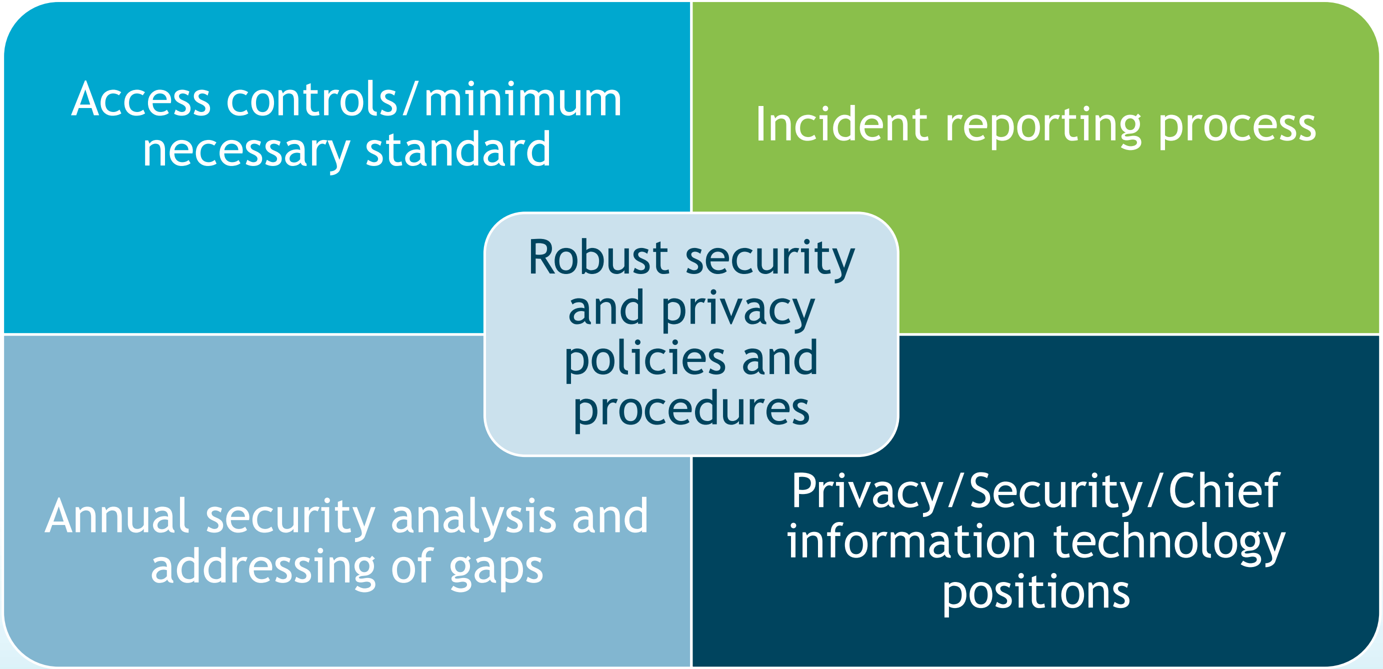
- Robust antivirus program with ongoing updates
- Firewalls
- Prohibit or screen external media and applications

Strategies/best practices to avoid and mitigate cyber risk

Access

- Secure servers and hardware
- Limit transport of hardware or devices with PHI
- Put policies/limitations/prohibiting access to high-risk sites in place
- Audit schedule of network access
- Prohibit software application by staff
- Consider and plan for environmental risks

Strategies/best practices to avoid and mitigate cyber risk



Access controls/minimum necessary standard

Incident reporting process

Robust security and privacy policies and procedures

Annual security analysis and addressing of gaps

Privacy/Security/Chief information technology positions

Strategies/best practices to avoid and mitigate cyber risk

Create and promote a cyber security culture

- Build in best practices
- Reduce variation and increase consistency
- Ensure and monitor compliance
- Assign accountability
- Provide ongoing training and staff education
- Be cognizant of email risks and phishing
- Ensure vendor compliance and due diligence are in place

Summary

Be familiar with HIPAA privacy and security policies in your organization

Understand patients' rights in relation to reviewing, requesting, and releasing PHI

Understand rules in relation to BAs, as well as the concept of minimum necessary standard

Be familiar with how any incidents or suspected breaches are reported

Be diligent in using best practices to avoid cyberattacks

Resources

- Cybersecurity Resource List (MedPro Group)
- Guideline: Medical Records Release (MedPro Group)
- Risk Q & A on Telehealth/Telemedicine (MedPro Group)
- Summary of the HIPAA Privacy Rule (Department of Health and Human Services)
- Summary of the HIPAA Security Rule (Department of Health and Human Services)
- Virtual Risk: An Overview of Telehealth from a Risk Management Perspective (MedPro Group)

Disclaimer

The information contained herein and presented by the speaker is based on sources believed to be accurate at the time they were referenced. The speaker has made a reasonable effort to ensure the accuracy of the information presented; however, no warranty or representation is made as to such accuracy. The speaker is not engaged in rendering legal or other professional services. If legal advice or other expert legal assistance is required, the services of an attorney or other competent legal professional should be sought.