HIPAA PASS
Privacy and Security Solutions

HIPAA Highlights and Impact to your Telehealth Program

Wednesday, Sept 27, 2017

mountain-pacific quality health
HEALTH TECHNOLOGY SERVICES
transforming health care through innovative technology

Susan Clarke, HCISPP

- (ISC)^2 certified Healthcare Information Security and Privacy Practitioner.
- 15+ years of Healthcare Experience.
- 10+ years design and development EHR software, BS with computer science major.
- National Incident Management Systems Certificate.
- Served on IT Security, Disaster Recovery and Joint Commission steering committee.
- Served as communications unit lead during Healthcare system’s ready and complete alerts.

Mountain-Pacific

Mountain-Pacific Quality Health is a private, non-profit, community-based organization that has dedicated more than three decades to improving health and health care in: Alaska, Hawaii (including some U.S. Pacific Territories), Montana and Wyoming. Our goal is to increase access to high-quality health care that is affordable, safe and of value to the patients we serve.

Mountain-Pacific

Mountain-Pacific recognizes that HIPAA compliance can place an excessive burden on small and medium sized organizations so we created HIPAA Privacy and Security Solutions to provide easy, affordable and comprehensive solutions for those who need us most.

Legal Disclaimer

The presenter is not an attorney and the information provided is the presenter(s)' opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar(s) and related materials (including, but not limited to, recordings, handouts, and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar(s) and webinar materials should not in any manner rely upon or construe the information as legal, or other professional advice. Users should seek the services of a competent legal or other professional before acting, or failing to act, based upon the information contained in the webinar(s) in order to ascertain what is may be best for the users individual needs.

Acronyms…

- BA: Business Associate
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare and Medicaid Services
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- HHS: Department of Health and Human Services
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- IT: Information Technology
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PHI: Protected Health Information
- SP: Special Publication
- SRA: Security Risk Analysis

Today's Overview

- HIPAA and Telehealth
- HIPAA Rules and who is Covered
- Business Associate and the Laws
- Privacy, Disclosures and Telehealth Considerations
- IT Security, Standards and Safeguards and Telehealth Considerations
- Insider Threat
- Breach, Enforcement and importance of Security Risk Analysis
- Take Aways and Resources
- Parting thought and Q&A

HIPAA and Telehealth

- Privacy, security, and confidentiality issues must be addressed in telemedicine the same as in conventional medical practices.
- Telemedicine increases the frequency that PHI is available electronically, challenge to keep ePHI confidential.
- Technical safeguards like encryption provide safe harbor.
- No control over vendors actions or operations, clearly state in Business Associate agreements.

PASS

Mobile Medical Apps and HIPAA

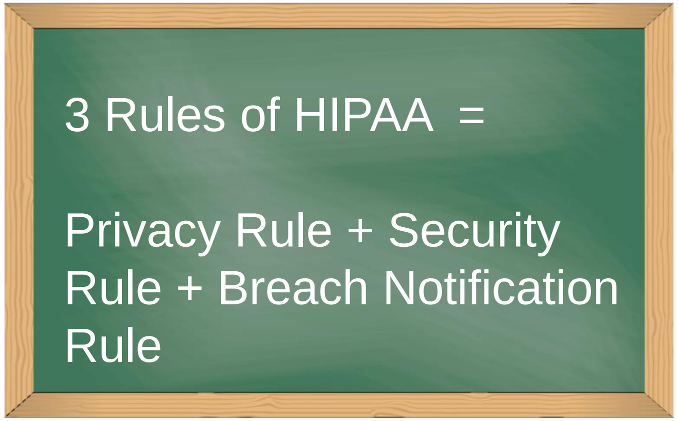
- Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software--think fitbit.
- There are many domains such as FTC privacy and fair practices, State privacy laws, consumer reporting agency.
- Mobile apps span a wide range of health functions, link to find out if regulated by FDA.

http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368743.htm

Who is Covered under HIPAA?

Covered Entities:

- Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
- Health plans
- Health care clearinghouses



3 Rules of HIPAA =

Privacy Rule + Security Rule + Breach Notification Rule

Business Associates:

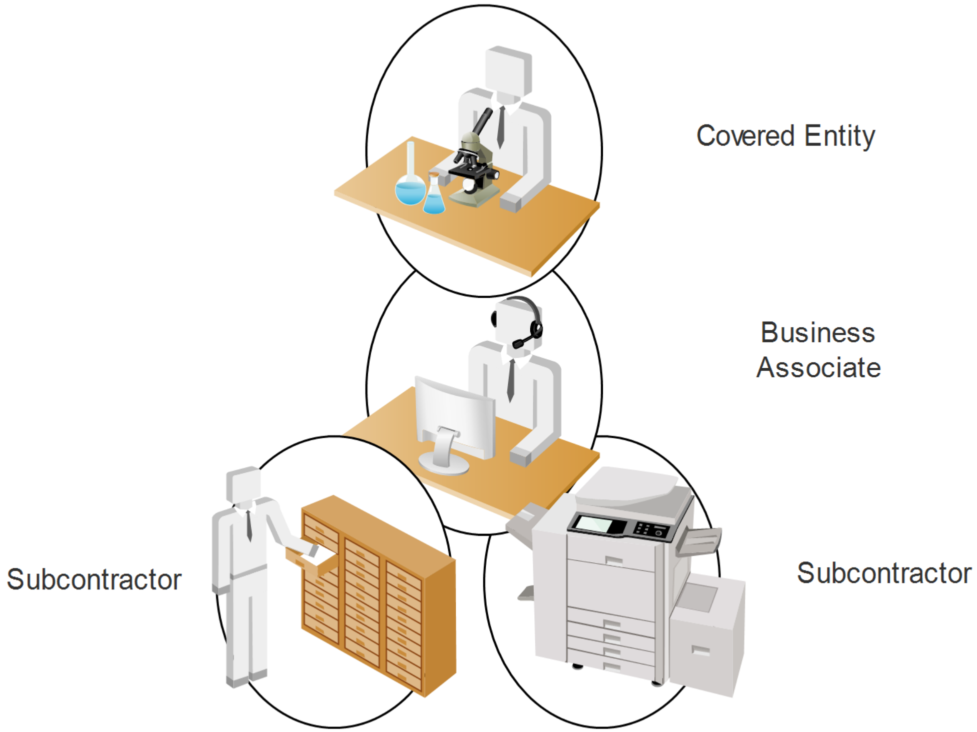
- Agents, contractors, and others hired to do the work of, or to work for, the covered entity, and such work requires the use or disclosure of protected health information

Business Associate

- Telehealth can have a greater number of platforms, role of telehealth company (BA) in data storage, reporting, billing.
- BAs must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; liable for Security Rule violations
- BA must comply with use or disclosure limitations expressed in its contract and those in the Privacy Rule; criminal and civil liabilities attach for violations
- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities

Subcontractors of a Business Associates are defined as a Business Associates

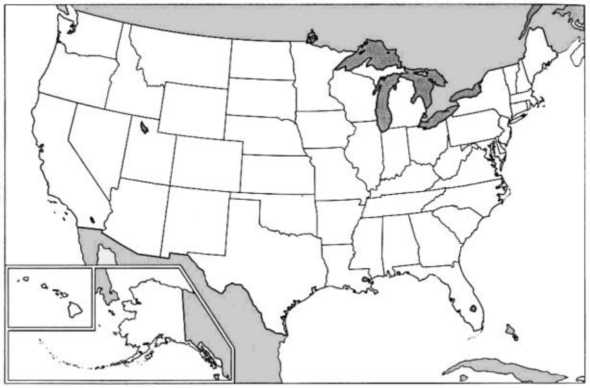
Chain of Trust



Important: Business Associate liability can flow to all subcontractors.

Telehealth State and Federal Laws

Sector/Jurisdiction specific, certain Providers or types of information. consumer protection laws, state breach reporting



State Laws

Federal Laws

HIPAA & HITECH

-Informed consent for telemedicine.
-Mental health information.
-Substance abuse information.
-HIV/AIDS/communicable disease data.
-Genetic data.
-Marketing restrictions.

Importance of Privacy

- People choose to disclose their most intimate information in order to get healthy
- Care providers earn their trust by guaranteeing privacy
- Privacy is assured by properly protecting systems and information
- Breaches undermine patient confidence
- No confidence and people avoid treatment, lie or omit information, opt-out and potentially get sicker
- Privacy and security are integral to care

Disclosures Not Permitted

The HIPAA Privacy Rule provides that Covered Entities or Business Associates may not use or disclose PHI except as permitted or required. See 45 C.F.R. §164.502(a). Examples of Potential Violations:

- Permits news media to film individuals in its facility prior to obtaining their authorization.
- Publishes PHI on its website or on social media without an authorization from the individual(s).
- Confirms that an individual is a patient and provides other PHI to reporter(s) without authorization from the individual.
- Faxes PHI to an individual’s employer without authorization from the individual.

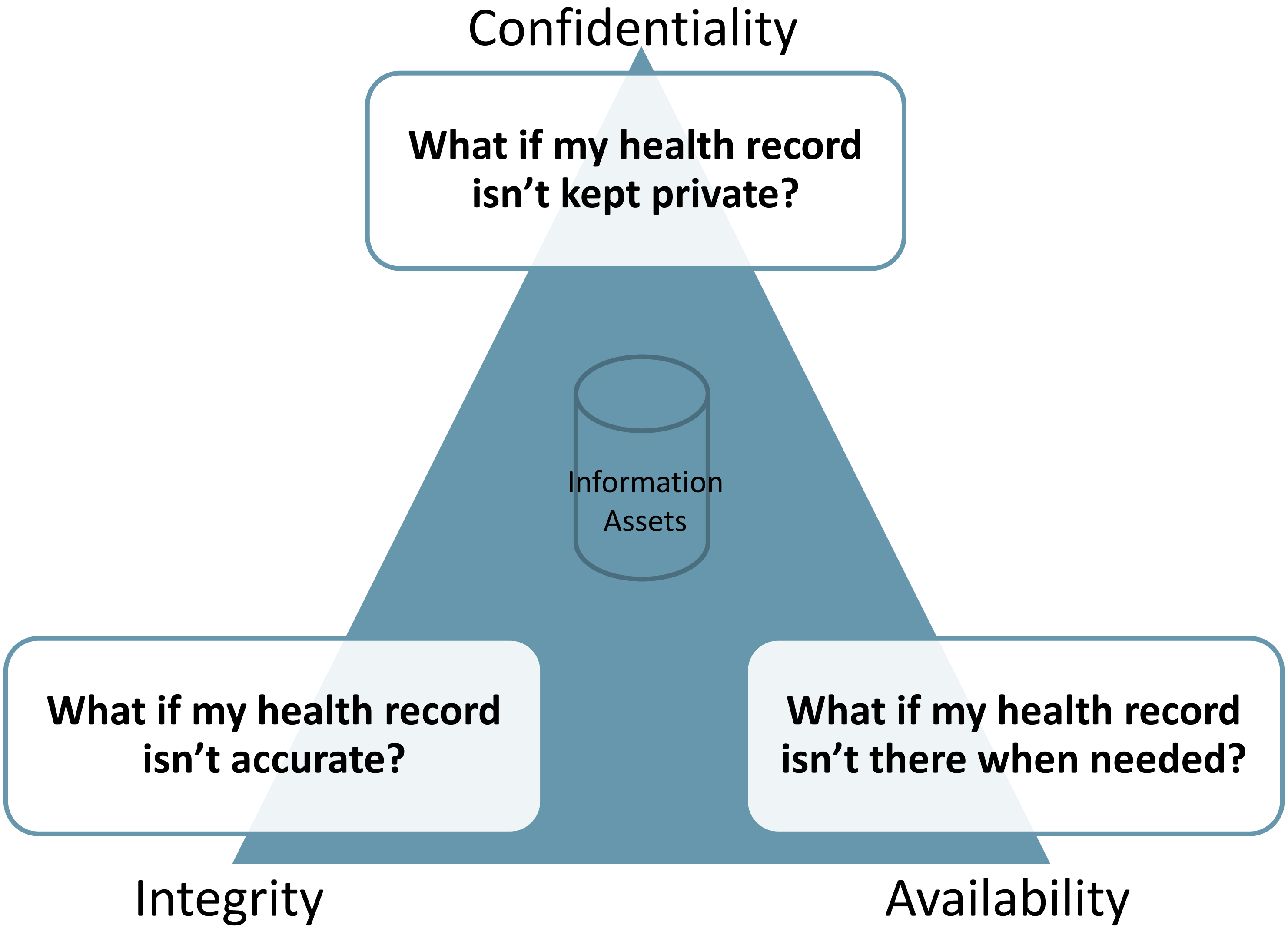
Telehealth Privacy Considerations

- Notice of Privacy Practices, Website Privacy Statement, Terms of Use, Online "pop-up" authorization, electronic signature, informed consent to Telemedicine.
- State laws vary, if multiple States use strictest to standardize processes.
- There must be a private and uninterrupted space in which the equipment is kept where the client/patient will consult with the provider.
- Providers and patients using televideo equipment often speak louder than normal.
- HIPAA laws that govern use, disclosure and breach must be followed faithfully.
- There should be a door that closes and is able to be locked.
- A telephone is needed as backup in case the televideo connection drops.

Telehealth Security Considerations

- Data Security including encryption, authentication and data storage.
- Challenge of protecting ePHI as it moves through the healthcare system.
- A robust IT department will support telehealth security requirements.
- Telehealth access to the local EHR, use of consumer data, deidentification for mining and re-sale.
- Some medications require a “wet signature”.
- Credentialing staff, this can be a lengthy process.
- Telehealth may be unfamiliar territory for security professionals.

IT Security & CIA Triad



Confidentiality

What if my health record isn’t kept private?

Information Assets

What if my health record isn’t accurate?

What if my health record isn’t there when needed?

Integrity

Availability

Unprecedented Security Risk
We need to take a team approach

- What is the operational consequence?
- What is the patient care consequence?
- What can happen to my organization?
- Can data being held hostage impact patient care?
- Have we underestimated the proliferation of ePHI within our environments.
- What is the cost of a breach?

There is no such thing as 100% security or zero risks.

Healthcare today is a hotbed for cybersecurity activity

Electronic Health Records + Sharing patient records across ecosystem + Data-based collaborative care + Analytics used to enhance care + Electronic registries for population health + Personalized Medicine

= Data Explosion!

Standards and Safeguards

- Standards
  - a covered entity (and business associate) must comply with the standards and specifications. Some specifications are required and some are addressable.
- Safeguards
  1. Administrative
  2. Technical
  3. Physical

Administrative Safeguards

- Administrative Safeguards
  - "…are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." (*Definitions - 45 CFR §164.304).*

Physical & Technical Safeguards

- Physical Safeguards
  - "…are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." (*Definitions - 45 CFR §164.304).*
- Technical Safeguards
  - "…means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." (*Definitions - 45 CFR §164.304).* ie active monitoring, two factor authentication, no unauthorized access.

Patching Software

- The use of unpatched or unsupported software on systems which access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software which should be monitored for patches and vendor end-of-life for support include router and firewall firmware
- Anti-virus and anti-malware software
- Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

Transmission Security

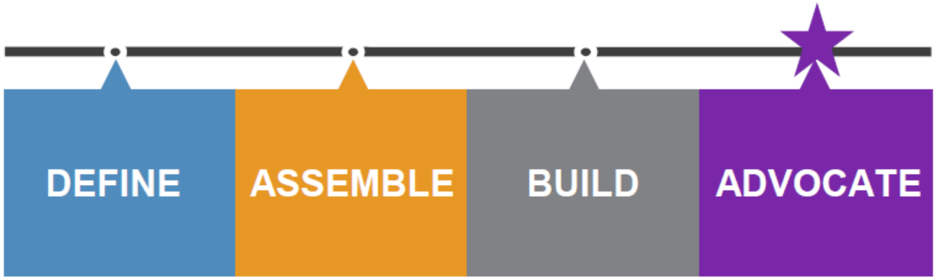
- Make sure encryption is both at rest and in motion. Some vendors don’t go through the extra step of making sure the data is encrypted as it is moving through the internet.
- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented whenever deemed appropriate. See 45 C.F.R. §164.312(e)(2)(ii).
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)

EHR on Mobile Devices: SP 1800-1

Secure exchange of electronic health information

Overview

- Medical identity theft costs billions each year, and altered medical information can put a patient's health at risk
- The use of mobile devices to store, access, and transmit electronic health records is outpacing the privacy and security protections on those devices
- This practice guide demonstrates how healthcare organizations can secure electronic health records on mobile devices using commercially available and open source products



DEFINE ASSEMBLE BUILD ADVOCATE

Project Status

Revising practice guide to publish final SP 1800-1

Collaborate with Us

- Read Securing Electronic Health Records on Mobile Devices Practice Guide
- Email hit_nccoe@nist.gov to join the Community of Interest for this project

Insider Treat

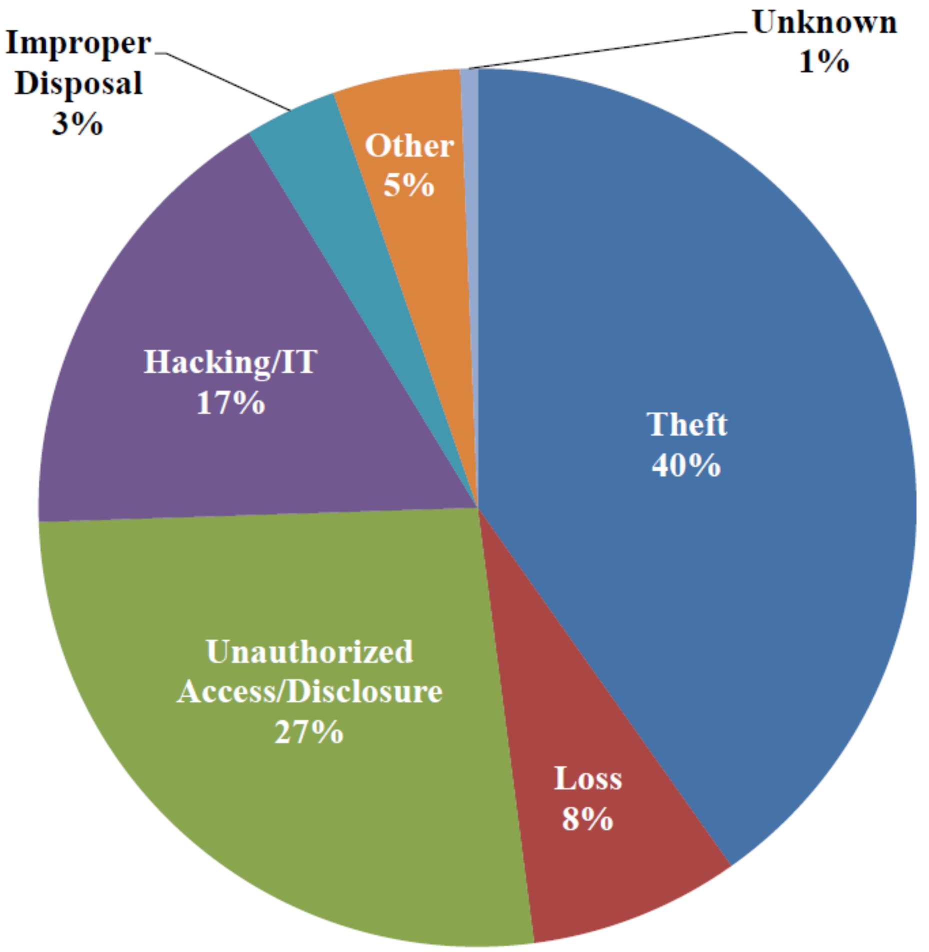
Insider threat is becoming one of the largest threats to organizations and some cyberattacks may be insider-driven. Although all insider threats are not malicious or intentional, the effect of these threats can be damaging to your organization. Safeguards are often more psychology than technology

According to a survey recently conducted by Accenture and HFS Research, 69% of organization representatives surveyed had experienced an insider attempt or success at data theft or corruption.

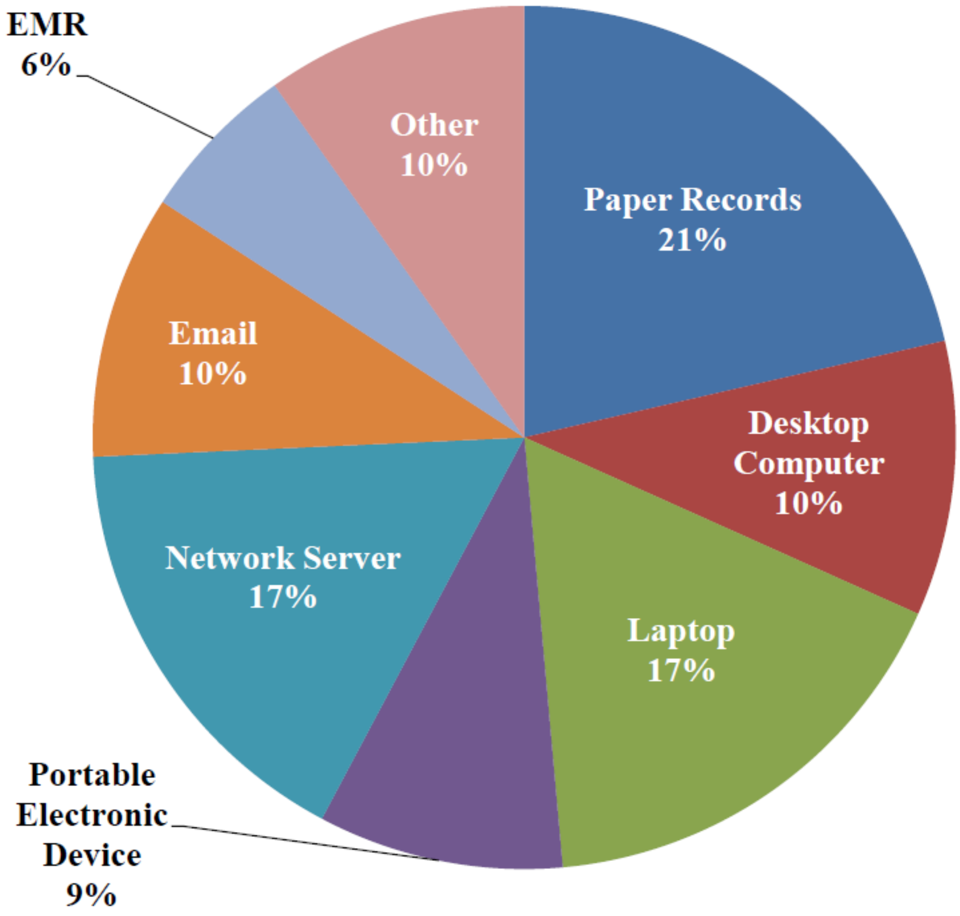
IMPORTANT: Both annual and ongoing training!

Source=Privacy-List listserv, operated by the Office for Civil Rights (OCR)

500+ Breaches by Type of Breach as of July 31, 2017



500+ Breaches by Location of Breach as of July 31, 2017



Recent Enforcement Actions

- https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html
- 5/23/2017: Careless handling of HIV information jeopardizes patient’s privacy
- 5/10/2017: Texas health system settles potential HIPAA violations for disclosing patient information
- 4/24/2017: Settlement shows that not understanding HIPAA requirements creates risk
- 4/20/2017: No Business Associate Agreement?
- 4/12/2017: Overlooking risks leads to breach
- 2/16/2017: HIPAA settlement shines light on the importance of audit controls
- 2/1/2017: Lack of timely action risks security and costs money
- 1/18/2017: HIPAA settlement demonstrates importance of implementing safeguards for ePHI

HIPAA Breach Highlights

September 2009 through July 31, 2017

- Approximately 2,017 reports involving a breach of PHI affecting 500 or more individuals
  - Theft and Loss are 48% of large breaches
  - Hacking/IT now account for 17% of incidents
  - Laptops and other portable storage devices account for 26% of large breaches
  - Paper records are 21% of large breaches
  - Individuals affected are approximately 174,974,489
- Approximately 293,288 reports of breaches of PHI affecting fewer than 500 individuals

Cybersecurity Newsletters

February 2016	Ransomware, "Tech Support" Scam, New BBB Scam Tracker
March 2016	Keeping PHI safe, Malware and Medical Devices
April 2016	New Cyber Threats and Attacks on the Healthcare Sector
May 2016	Is Your Business Associate Prepared for a Security Incident
June 2016	What's in Your Third-Party Application Software
September 2016	Cyber Threat Information Sharing
October 2016	Mining More than Gold (FTP)
November 2016	What Type of Authentication is Right for you?
December 2016	Understanding DoS and DDoS Attacks
January 2017	Audit Controls
February 2017	Reporting and Monitoring Cyber Threats
April 2017	Man-in-the-Middle Attacks and "HTTPS Inspection Products"

http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Perform a Security Risk Analysis

- Conducting a security risk analysis is a process of identifying, estimating, and prioritizing information security risks that could compromise the Confidentiality, Integrity and Availability of protected health information in a health care facility. *See 45 C.F.R. § 164.308(a)(1)(ii)(A).*
- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.
- Examples: EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); removable media

Important Links on hhs.gov

Privacy rule:

http://www.hhs.gov/hipaa/for-professionals/privacy/

Security rule:

- http://www.hhs.gov/hipaa/for-professionals/security/

Business Associate:

- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

Breach Notification Rule:

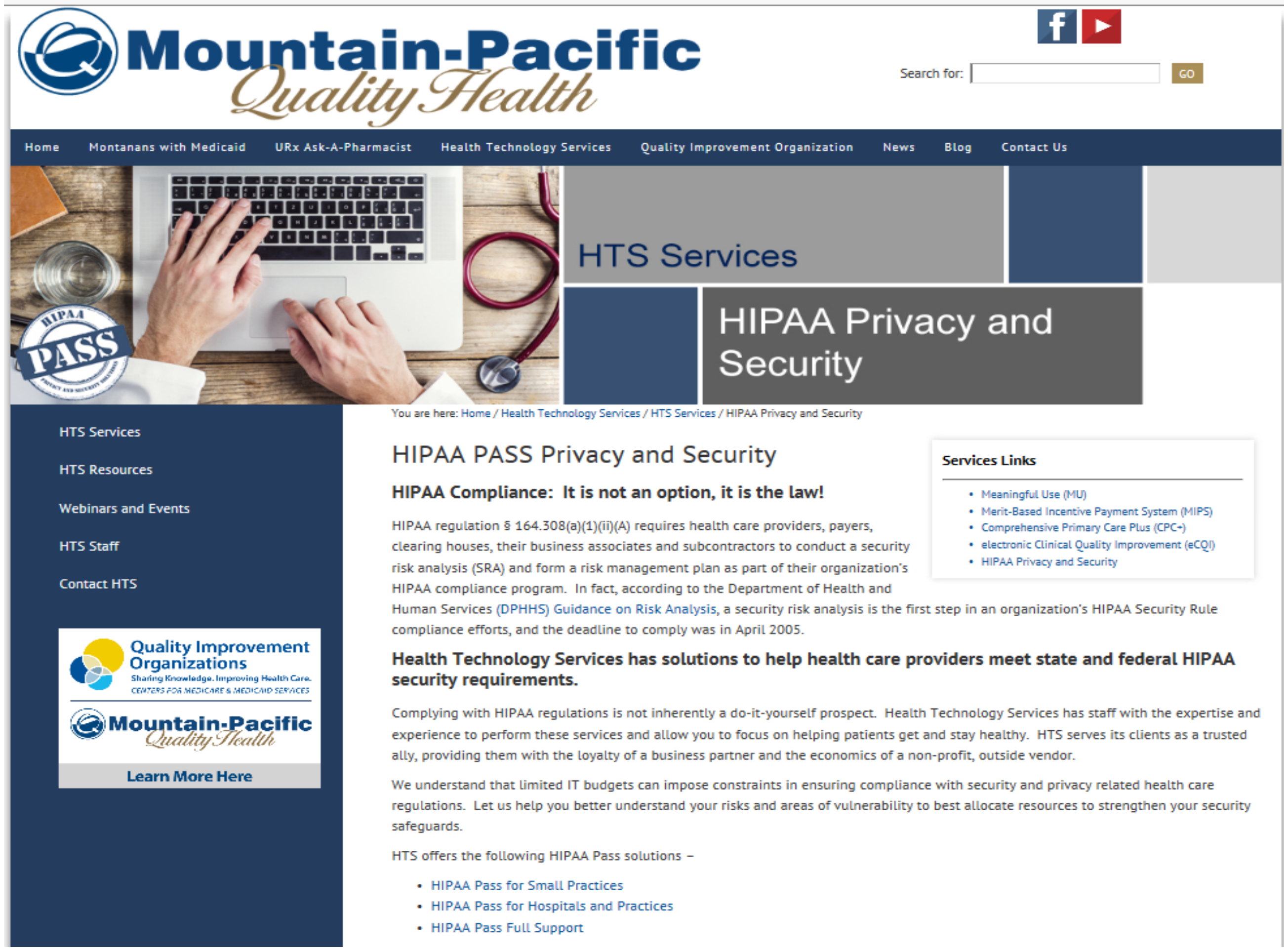
- http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

A parting thought…

Please always remember that checking the box for compliance is important, and protecting patients and their health records is even more important.

Thanks for your valuable time today.

http://mpqhf.com/corporate/health-and-technology-services/hts-services/hipaa-privacy-and-security/


Mountain-Pacific Quality Health
Search for:
GO
Home
Montanans with Medicaid
URx Ask-A-Pharmacist
Health Technology Services
Quality Improvement Organization
News
Blog
Contact Us
HIPAA PASS
HTS Services
HIPAA Privacy and Security
HTS Services
HTS Resources
Webinars and Events
HTS Staff
Contact HTS
Quality Improvement Organizations
Sharing Knowledge. Improving Health Care.
CENTERS FOR MEDICARE & MEDICAID SERVICES
Mountain-Pacific Quality Health
Learn More Here

You are here: Home / Health Technology Services / HTS Services / HIPAA Privacy and Security

HIPAA PASS Privacy and Security

Services Links

- Meaningful Use (MU)
- Merit-Based Incentive Payment System (MIPS)
- Comprehensive Primary Care Plus (CPC+)
- electronic Clinical Quality Improvement (eCQI)
- HIPAA Privacy and Security

HIPAA Compliance: It is not an option, it is the law!

HIPAA regulation § 164.308(a)(1)(ii)(A) requires health care providers, payers, clearing houses, their business associates and subcontractors to conduct a security risk analysis (SRA) and form a risk management plan as part of their organization's HIPAA compliance program. In fact, according to the Department of Health and Human Services (DPHHS) Guidance on Risk Analysis, a security risk analysis is the first step in an organization's HIPAA Security Rule compliance efforts, and the deadline to comply was in April 2005.

Health Technology Services has solutions to help health care providers meet state and federal HIPAA security requirements.

Complying with HIPAA regulations is not inherently a do-it-yourself prospect. Health Technology Services has staff with the expertise and experience to perform these services and allow you to focus on helping patients get and stay healthy. HTS serves its clients as a trusted ally, providing them with the loyalty of a business partner and the economics of a non-profit, outside vendor.

We understand that limited IT budgets can impose constraints in ensuring compliance with security and privacy related health care regulations. Let us help you better understand your risks and areas of vulnerability to best allocate resources to strengthen your security safeguards.

HTS offers the following HIPAA Pass solutions –

- HIPAA Pass for Small Practices
- HIPAA Pass for Hospitals and Practices
- HIPAA Pass Full Support

Please let me know how I can help?

Contact information:

Susan Clarke, sclarke@mpqhf.org, (307) 248-8179