Career Development Series 2024

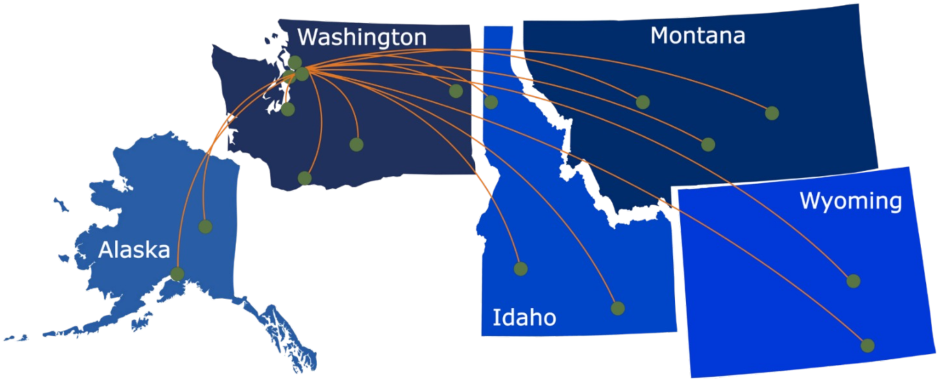
Protecting Privacy and Maintaining Security in Telemedicine

ITHS | Institute of Translational Health Sciences
ACCELERATING RESEARCH. IMPROVING HEALTH.

UNIVERSITY of WASHINGTON

FRED HUTCH
CURES START HERE

Seattle Children's
HOSPITAL · RESEARCH · FOUNDATION



What We Offer:

1. Research Support Services: Members gain access to the different research services, resources, and tools offered by ITHS, including the ITHS Research Navigator.

2. Community Engagement: Members can connect with regional and community based practice networks

3. Education & Training: Members can access a variety of workforce development and mentoring programs and apply for formal training programs.

4. Funding: Members can apply for local and national pilot grants and other funding opportunities. ITHS also offers letters of support for grant submissions.

Contact ITHS

Director of Research Development

- Project Consultation
- Strategic Direction
- Resources and Networking

Melissa D. Vaught, Ph.D.
ithsnav@uw.edu
206.616.3875

Scientific Success Committee

- Clinical Trials Consulting
- Guidance on Study Design, Approach and Implementation
- Feedback on Design and Feasibility

https://www.iths.org/investigators/services/clinical-trials-consulting/

Feedback

At the end of the seminar, a link to the feedback survey will be sent to the email address you used to register.

Telemedicine 2.0 Series

Date	Session	Title
	Session 1	Telemedicine 2.0: How Is It Relevant to Me? (Pre-recorded video available)
Sept. 25, 2024	Session 2	Telehealth Then and Now
Oct. 1, 2024	Session 3	Telemedicine Regulatory Issues: Licensing, Standards of Practice, Billing, and Reimbursement
Oct. 8, 2024	Session 4	Protecting Privacy and Maintaining Security in Telemedicine
Oct. 15, 2024	Session 5	The Entrepreneur’s Perspective on Telemedicine Technology and Tools Development
Oct. 24, 2024	Session 6	Digital Inclusion and Access to Care by Telemedicine

More details at: https://www.iths.org/event/telemedicine-then-and-now/?instance_id=1372

Telemedicine 2.0 Series – Learning Objectives

At the end of the series, participants will be able to:

1. Identify opportunities to improve remote patient care

2. Identify security and privacy risks associated with telemedicine technologies

3. Mitigate introduction of disparities in access to clinical care

Career Development Series 2024

Protecting Privacy and Maintaining Security in Telemedicine

Session 4

Presented by:

Joseph “Augie” D’Agostino,
MEd, CISO

Lenny Sanchez,
JD, CHC

ITHS | Institute of Translational Health Sciences
ACCELERATING RESEARCH. IMPROVING HEALTH.

Disclosures

Today’s speaker has no financial relationships with an ineligible company relevant to this presentation to disclose.

UW Medicine
UW SCHOOL
OF MEDICINE

None of the planners have relevant financial relationship(s) to disclose with ineligible companies whose primary business is producing, marketing, selling, re-selling, or distributing healthcare products used by or on patients

All relevant financial relationships have been mitigated

Session 4 Learning Objectives

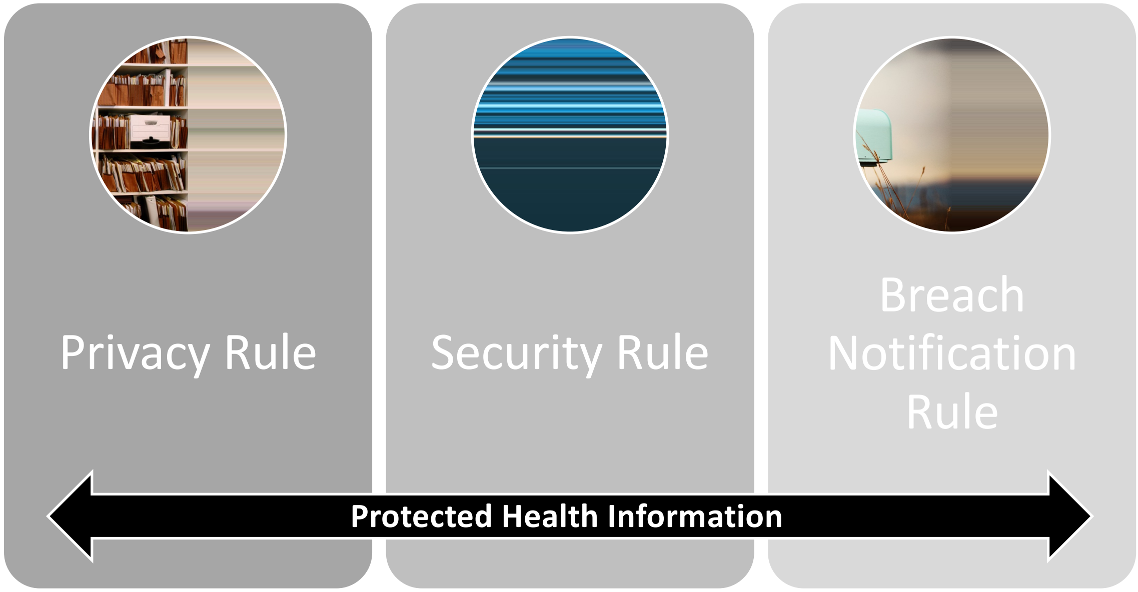
At the end of the session, participants will be able to:

1. Understand the intersection of patient privacy principles with telemedicine

2. Understand the basics of telemedicine cybersecurity controls

3. Understand threats unique to telemedicine and personal and device hygiene habits to mitigate such threats

What is HIPAA?



Privacy Rule

Security Rule

Breach Notification Rule

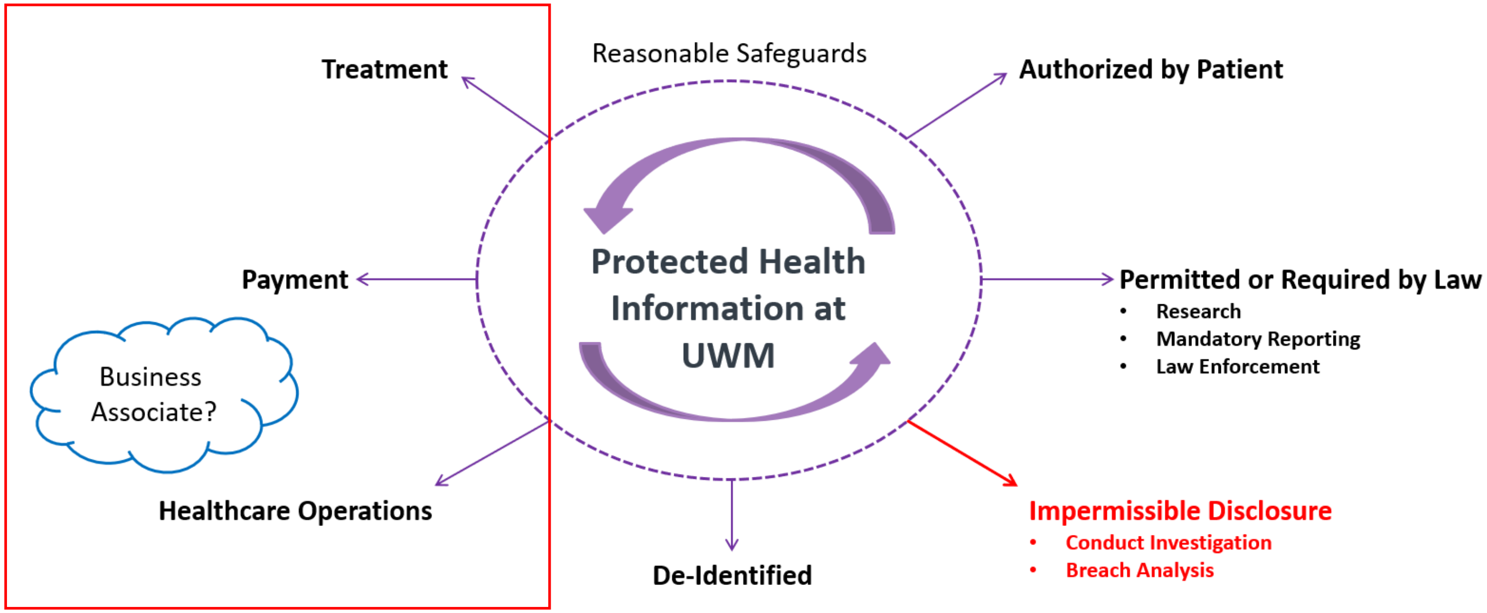
Protected Health Information

- Applies to “covered entities”: healthcare providers, health insurance companies, and healthcare clearinghouses
- Creates standards for privacy and security of “protected health information” (PHI)
- Articulates how covered entities may use and disclose PHI

What is Protected Health Information?

- Protected Health Information (PHI) is defined as information created, stored or received by a HIPAA covered entity that relates to a patient’s physical or mental health care.
- PHI can be verbal, written or electronic (ePHI)
- The information must:
  - Identify the patient, or
  - Provide a reasonable basis to believe the information can be used to identify the patient.

HIPAA Privacy Rule



Reasonable Safeguards

Protected Health Information at UWM

Treatment

Payment

Business Associate?

Healthcare Operations

Authorized by Patient

Permitted or Required by Law

- Research
- Mandatory Reporting
- Law Enforcement

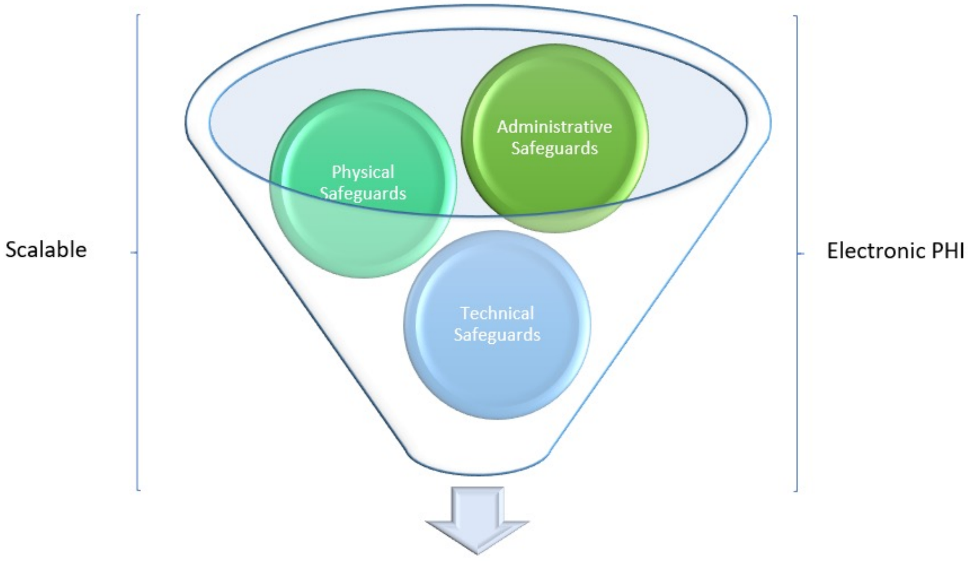
De-Identified

Impermissible Disclosure

- Conduct Investigation
- Breach Analysis

HIPAA Security Rule

- Designed to reduce the risks and vulnerabilities to ePHI through the adoption of administrative, physical and technical safeguards
- Requirements flow down to Business Associates; memorialized in BAA
- HIPAA does not allow BAs to use PHI prohibited by Privacy Rule or apply safeguards below Security Rule standards

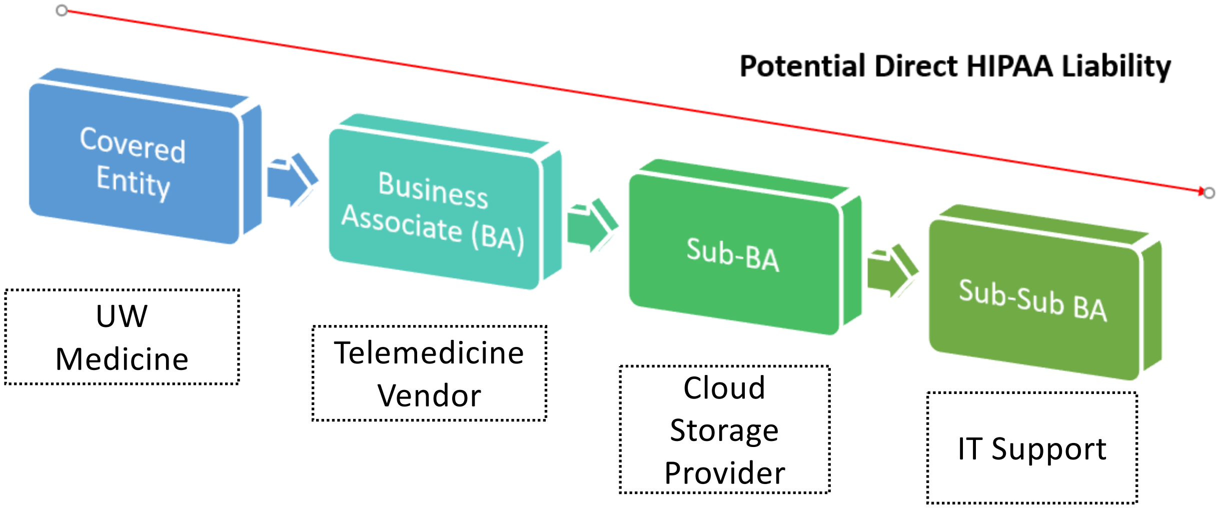


“HIPAA Compliant”

Business Associates

What is a "Business Associate"?

1. An entity that is not a part of the HIPAA covered entity;
2. That performs a service or activity for or on behalf of the covered entity; and
3. That involves the use or disclosure of PHI.



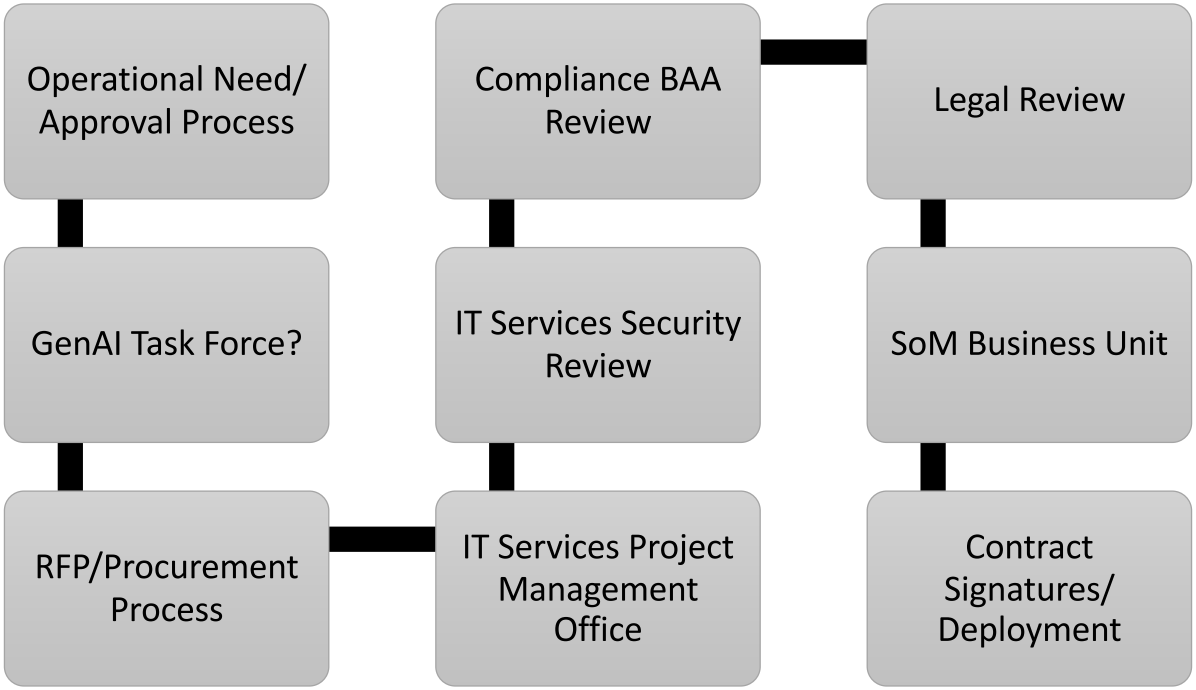
Healthcare Providers & Vendors

- Does the vendor understand the limitations re: PHI usage?
  - Treatment, payment and healthcare operations – generally supports the healthcare provider’s business
  - Use of PHI to develop the vendor’s product/service

- Does the vendor seek to de-identify the healthcare provider’s PHI?
  - True ability to de-identify data
  - Data can be used without Privacy Rule restrictions
  - Healthcare provider’s loss of control over data

- Does the healthcare provider trust the vendor with patient data?

Adoption of Vendor Solution at UW Medicine



Operational Need/ Approval Process

GenAI Task Force?

RFP/Procurement Process

IT Services Project Management Office

IT Services Security Review

Compliance BAA Review

Legal Review

SoM Business Unit

Contract Signatures/ Deployment

A CYBER SECURITY PERSPECTIVE

Areas we will cover:

- Telemedicine cybersecurity controls
- Threats to Telemedicine
- Personal and device hygiene in Telemedicine

Telemedicine Cybersecurity Controls

Telemedicine is being used more and more in the world’s changing technology landscape. The expansion of network connectivity and upgraded hardware and software expands the scope of medical centers patient delivery systems.

This expanding environment requires robust cybersecurity controls, including but not limited to:

- Access controls (User, network, and physical)
- Multi-factor Authentication
- Virtual Private Networks
- Endpoint protections

Telemedicine Cybersecurity Controls

Access controls and Multi-factor Authentication (MFA)

- As we know, unauthorized access is a major problem for anyone who uses a computer or high-tech devices such as smartphones or tablets, and one of the most common ways that hackers break into computers is by capturing passwords.

- Multi-factor authentication (MFA) is a security process that requires users to provide two or more pieces of evidence to verify their identity. This can include something they know, such as a password, and something they have, such as a physical security token or their fingerprint.

Telemedicine Cybersecurity Controls

VPN and End Point Protections

- Virtual Private Network (VPN): Using a VPN encrypts your internet traffic, preventing hackers from intercepting sensitive such as login credentials and personal information.

- End Point Protection: Is a crucial line of defense in the modern cybersecurity landscape. It goes beyond traditional antivirus software by continuously monitoring devices endpoints -- laptops, servers, and workstations for malicious activity to detect and respond to cyber threats like ransomware and malware

Threats to Telemedicine

The threat landscape for Telemedicine is very similar to other healthcare environments. The devices, applications, and software used must be maintained at the same high-level and all transmissions must be secured.

- Devices must be patched and kept up to date.
- Applications must be patched, and access limited to least privilege.
- All transmissions must be encrypted using an approve encryption method.

Personal and Device Hygiene in Telemedicine

Hygiene is very important in any healthcare setting. When conducting Telemedicine visits it is even more important due to the unknown nature of the environment.

- Personal hygiene – Unlike a medical center or other healthcare environment, a clinician or support staff member could bring unknown issues into a telemedicine environment if they are not very careful with every aspect of the process. From transportation to what they have on their person.

- Device Hygiene – Devices used for Telemedicine must go through the same stringent hygiene controls that any device in other healthcare environments go through. These devices are mobile and move through multiple non-hygienic spaces.

Thank You!

Open for Questions

ITHS | Institute of Translational Health Sciences

ACCELERATING RESEARCH. IMPROVING HEALTH.

Feedback Survey

A link to the feedback survey has been sent to the email address you used to register.

Please get out your device, find that email, and spend a few moments completing that survey before you leave today.

Tip: If on a mobile device, shift view to landscape view (sideways) for better user experience.