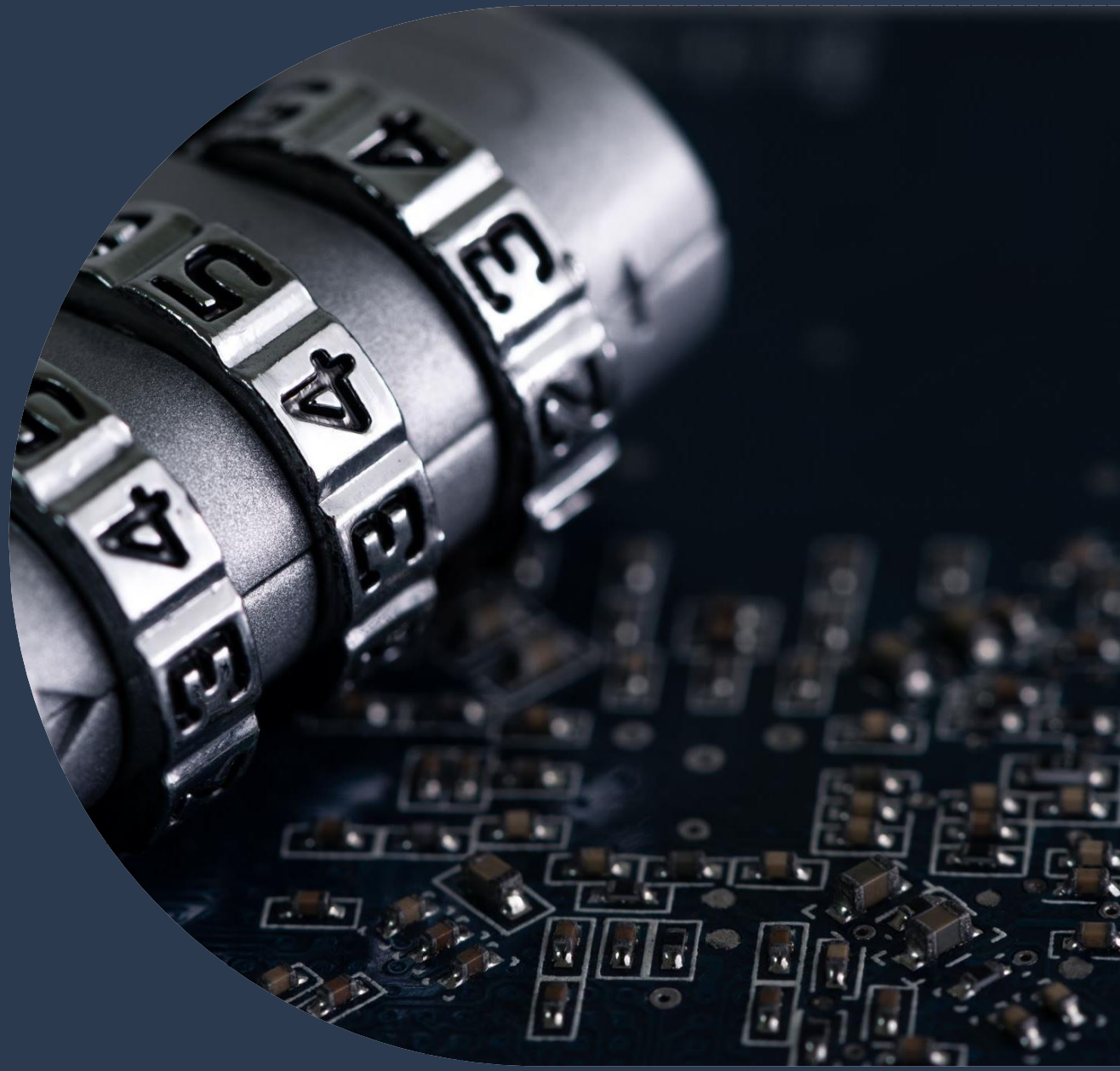
Lifeworks Privacy and Security

Compliance and IT Department



To support the services we provide, Lifeworks is required to collect personal information about individuals

Lifeworks is a covered entity and is required to comply with how private information is used, disclosed, and protected:

Federal Health Insurance Portability and Accountability Act (HIPAA)

Minnesota Government Data Practices Act (MGDPA)

Contractual Agreements

Privacy Rule

The HIPAA Privacy Rule determines how we use, disclose, protect, and access information which qualifies as Protected Health Information.

The rule also allows certain privacy rights to the individual.

Privacy Rule

What is Protected Health Information?

Protected Health Information (PHI)

PHI is individual health information which is accessed, created, modified, received, or maintained by Lifeworks or Lifeworks Personnel in any form.

PHI includes information that either independently or collectively could be used to individually identify a person

PHI information includes:

- Medical
- Financial
- Demographic
- Social Security Number
- First and last name
- Date of Birth
- Service date (admission, death, discharge)
- Medical number

PHI information continued:

- Address
- Type of service
- Phone number
- Photographic image
- Internet Uniform Resource Locator (URL)
- Internet Protocol address (IP)
- Other unique identifiers that can be attributed to a specific individual
- Individual PHI is used by all Lifeworks departments due to the services and associated government or insurance funding

What is the Security Rule?

HIPAA Security Rule focuses on administrative, technical, and physical safeguards specifically as they relate to Electronic Protected Health Information (ePHI)

The HIPAA Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of ePHI

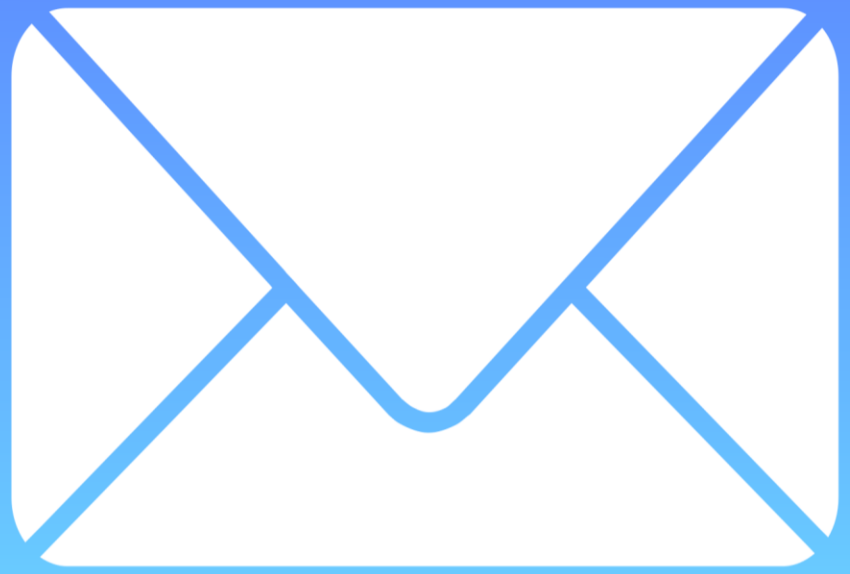
Security Rule continued…

Protection of ePHI data from unauthorized access whether external or internal, stored or in transit.

Examples: Breach attempts from phishing attacks or unauthorized access, destruction, or ransomware, to records or systems internally or externally

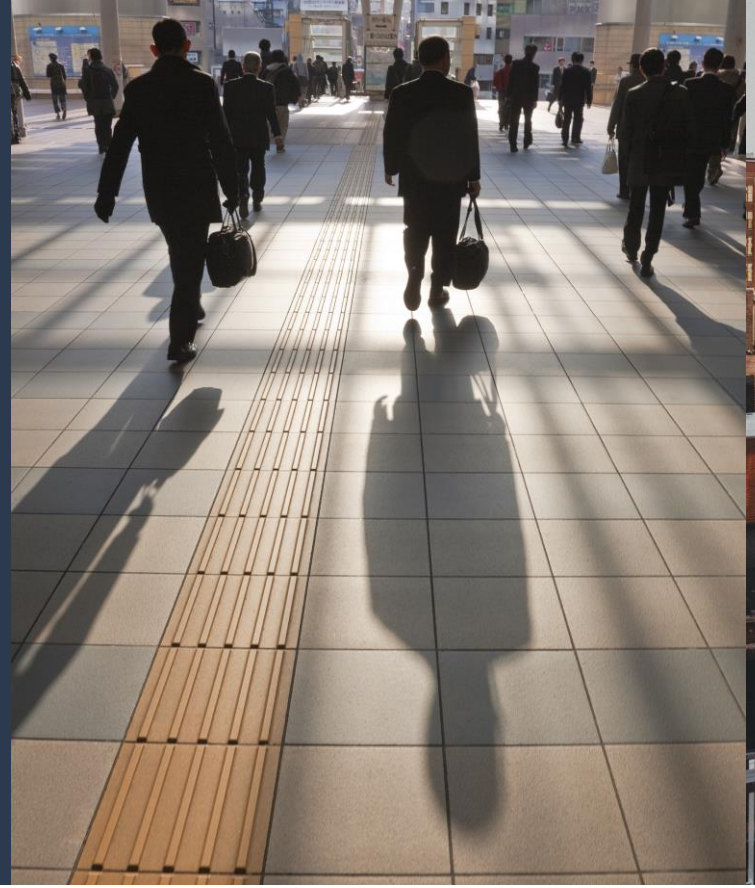
Security practices include:

- Secure encryption of emails
- Laptop or computer locking screen
- Requirements in passwords
- Firewalls
- Security assessments



- Email phishing testing
- Citrix desktop locking screen
- Phones password protected
- Vulnerability & patch management

Applying the Privacy and Security Rule in the community



01

Always be aware of your surroundings and what you are discussing.

02

PHI should not be discussed in open spaces. Find a private space to discuss.

03

Never leave your laptop and mobile phone out of your control. Keep these items in your possession.

Applying the Privacy and Security Rule in the community continued…

- Be aware of unknown and untrusted WIFI networks
- Lifeworks policies require all paper, including documents must be shredded. Use an approved Lifeworks shredder or use a shredder at a Lifeworks location
- All physical documents should be in your control or locked secured when you are not present
- Always utilize headphones for meetings on computer or laptop when in public or community spaces

Applying the Privacy and Security Rule in a Lifeworks setting

Minimum Necessary Rule:
Only accessing and using PHI information required to accomplish work-related task.

Discussions involving PHI should always apply the Minimum Necessary Rule

Keep confidentiality in mind when you are working in open spaces

Applying the Privacy and Security Rule in a Lifeworks setting continued...

- Utilize private spaces, when possible, to discuss PHI
- Always use headphones for meetings on computers when in communal spaces
- Verify individuals are authorized to receive PHI before releasing information
- Lifeworks clean desk policy:
  - Lock the screen of your computer and Citrix desktop when you will be away from it
  - Documents should be in your control or stored away
    - Lifeworks will provide locking option
  - Use electronic documentation, when possible, to limit printing documents
  - Information should not be left out when you are away

These practices include when working from home

Treat the privacy and security of participant Protected Health Information exactly how you would want your sensitive data to be treated.

Contact Us

IT Security

Specific questions to IT security, please open a Freshservice ticket

Don Becchetti- Director of Operations
dbecchetti@lifeworks.org

Mahamoud Warsame- Infrastructure Security Specialist
mwarsame@lifeworks.org

Compliance Department

Andrea Lang- Quality and Compliance Manager
alang@lifeworks.org

Sara Holeman- Compliance Technician
sholeman@lifeworks.org

Thank You!