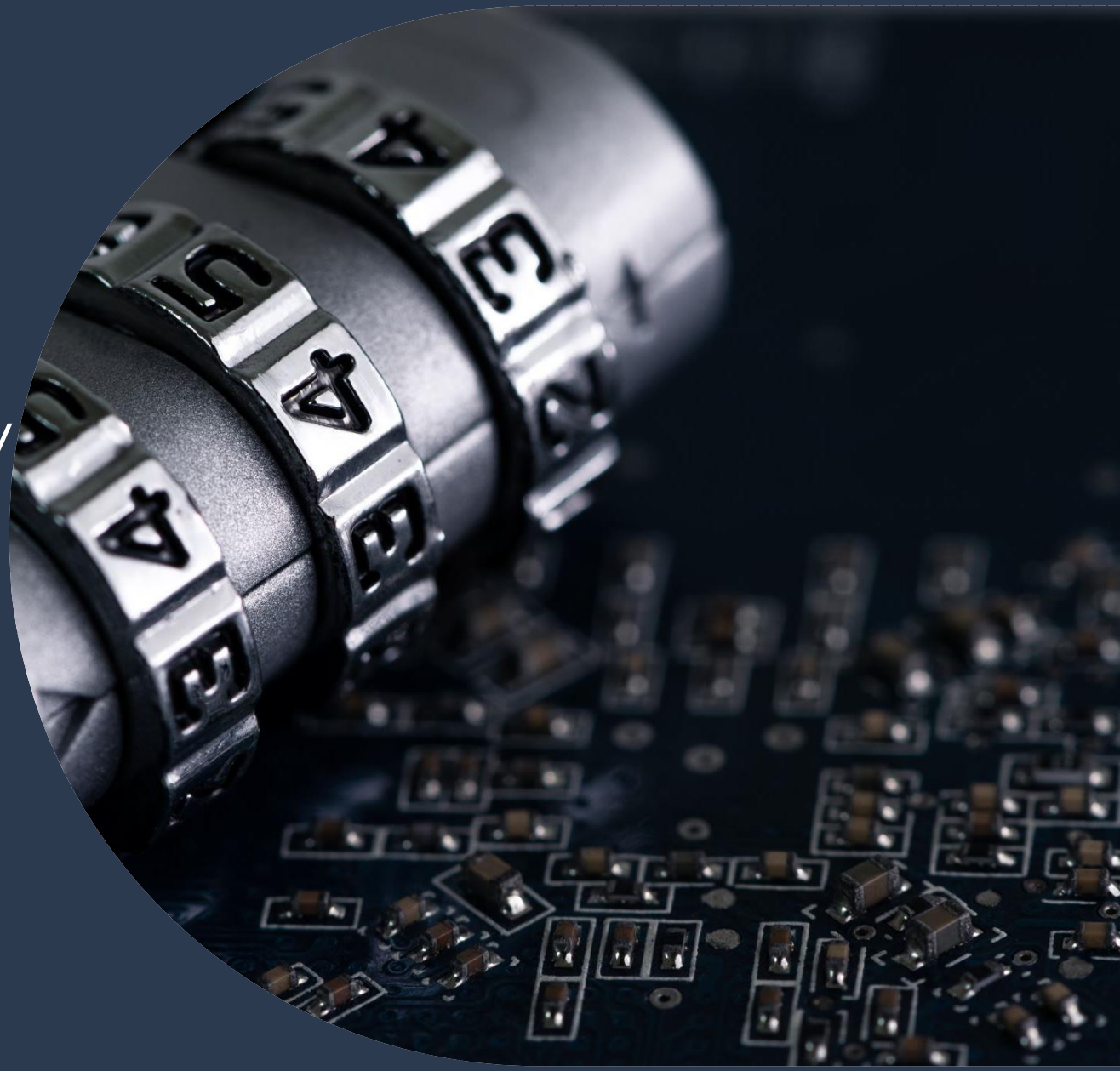
Lifeworks Privacy and Security

Compliance and IT Department



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

Lifeworks is required to comply with many laws, rules, and agreements on how private information is used, disclosed, and protected:

Federal Health Insurance Portability and Accountability Act (HIPAA)

Minnesota Government Data Practices Act (MGDPA)

Contractual Agreements

HIPAA Privacy Rule

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

The rule also allows certain privacy rights to the individual.

HIPAA 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 examples:

- Medical information
- Financial information
- Demographic information
- Social Security Number (SSN)
- First and last name
- Date of birth
- Service dates (admission, death, discharge)
- Medical Assistance (MA) number

PHI examples continued:

- Address
- Type of service
- Phone number
- Photographic image
- Internet Uniform Resource Locator (URL)
- Internet Protocol (IP) address
- 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.

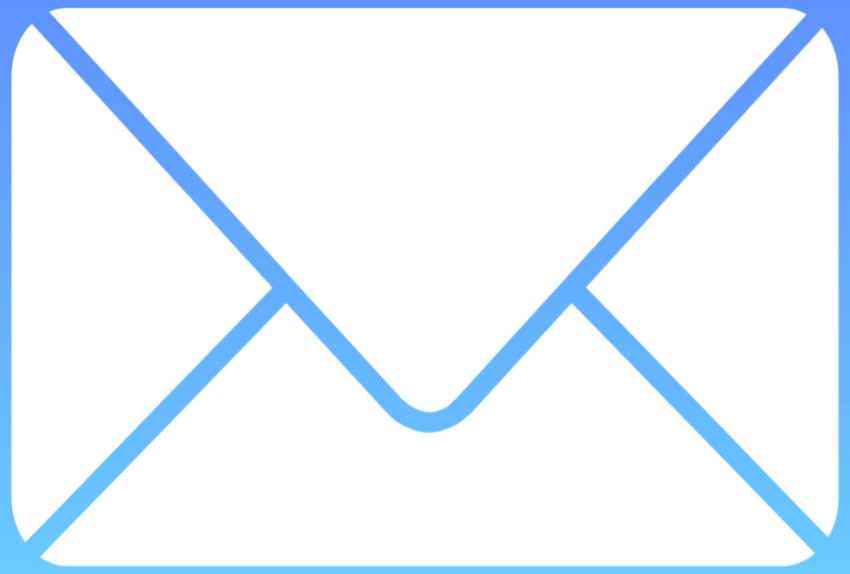
Security Rule continued...

The Security Rule ensures protection of ePHI data from unauthorized access whether external or internal, stored or in transit.

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

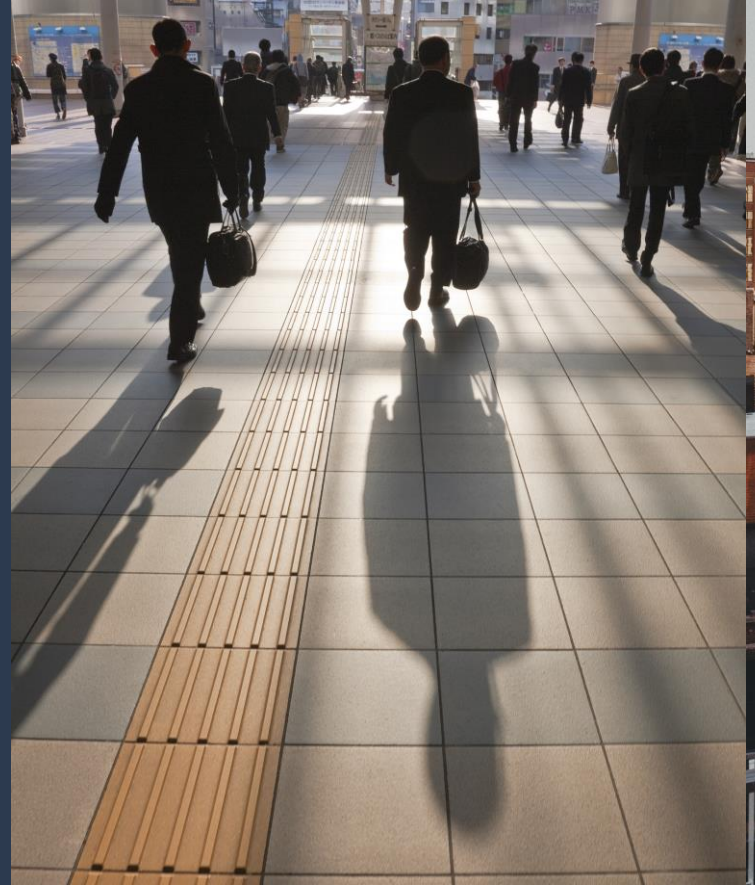
Security practices include:

- Secure encryption of emails- Outlook Encrypt button
- Laptop or computer locking screen
- Password standards
- Firewalls
- Security assessments



- Email phishing testing
- Citrix desktop locking screen
- Password protected phones
- Vulnerability and patch management

Applying the Privacy and Security Rules 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 or mobile device out of your control. Keep these items in your possession.

Applying the Privacy and Security Rules in the community continued…

- Be aware of unknown and untrusted Wi-Fi networks.

- Lifeworks policies require all paper documents must be shredded.
  - At a Lifeworks location, place ALL paper to be discarded in the Iron Mountain secure shredding bins.

  - All Personnel working from home, or other remote information technology locations, must have direct access to a Lifeworks provided cross-cut shredder or return for proper disposal at a Lifeworks controlled facility.

Applying the Privacy and Security Rules in the community continued…

- All physical documents should be in your control or locked secured when you are not present
- Always utilize headphones for meetings on Lifeworks devices when in public or community spaces
- Only use Lifeworks provided email, computing devices, and mobile devices to transmit and store client data

Applying the Privacy and Security Rules in a Lifeworks setting

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

Discussions involving PHI you should always apply the Minimum Necessary Rule

Keep confidentiality in mind when you are working in open spaces

Applying the Privacy and Security Rules in a Lifeworks setting continued…

- Utilize private spaces 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 storage option
  - Use electronic documentation to limit printing documents
  - Data on paper documents must not be visible when you are away from your working space

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.

Polices can be found:
SharePoint
LMS
Employee Handbook

Contact Us

Information Security Privacy Office:

Specific questions to IT security, please open a case: D365-IT@lifeworks.org

Don Becchetti
Operations Director

Matt Moore
IT Manager

Mahamoud Warsame
Infrastructure Security Specialist

Specific privacy questions to Compliance, please open a case: D365-Compliance@lifeworks.org

Andrea Lang
Quality and Compliance Manager

Sara Holeman
Compliance Technician

Thank You!