LifeWORKS
A nonprofit serving people with disabilities

Privacy and Security Policies Training

1

Lifeworks Compliance and IT Departments

This Training Includes:

- Introduction to Privacy and Security
- Acronyms
- Lifeworks Privacy Policies
- Lifeworks Security Policies
- Resources and Contact Information

Introduction

- To provide effective services to persons served, we collect certain health information about them that is very personal and private
- There are federal (HIPAA) and state (MGDPA) laws that dictate how we use, disclose, and protect that private information

Acronyms

- **HIPAA:** Health Insurance Portability and Accountability Act
- **HITECH:** Health Information Technology for Economic and Clinical Health
- **PHI:** Protected Health Information
- **ePHI:** Electronic Protected Health Information
- **MGDPA:** Minnesota Government Data Privacy Act
- **BAA:** Business Associate Agreement
- **BA:** Business Associate
- **CE:** Covered Entity
- **NPP:** Notice of Privacy Practices
- **OKR:** Organizational Knowledge Repository

What is Protected Health Information?

Protected Health Information (PHI) is:

- Health information about an individual (including clinical, financial, demographic related information) which is accessed, created, modified, received or maintained by Lifeworks or Lifeworks Personnel (in any form or media, whether electronic, oral, or paper) and which independently or collectively could be used to individually identify a person served

Common PHI for Lifeworks and persons served:

- Name, SSN, photo, date of birth, address, telephone #, diagnosis, type of service/treatment

Protected Health Information (PHI)

- Name
- Dates: birth, admissions, discharge, death
- Gender
- Medical records number
- Health plan beneficiary numbers
- Geographical subdivision smaller than a state (address, zip code, etc.)
- Phone number, email address, fax number
- License numbers
- Vehicle identification numbers (such as license plate numbers)
- Full face photographic images (and any comparable images)
- Social Security Number
- Device identifiers (such as serial numbers)
- URL (Internet Uniform Resource Locator)
- Internet Protocol (IP) address
- Biometric identifiers (such as fingerprints and voiceprints)
- Other unique identifiers that can be attributed to a specific individual

Lifeworks Privacy Policies

Define how PHI should be protected, used, disclosed, and accessed

What is the Privacy Rule?

- The Privacy Rule is a part of HIPAA that defines how **PHI** should be protected, used, disclosed, and accessed
- Establishes national privacy standards
- Sets boundaries on the uses and disclosures of PHI
- Provides certain privacy rights to individuals
- In situations when both the federal and the state privacy laws apply but appear to be conflicting, Lifeworks must comply with the **more stringent** of the two laws

HIPAA vs. MGDPA

Lifeworks abides by the MGDPA rule as it is more stringent

Authorizations

- HIPAA requires a one time consent permitting disclosures for treatment, payment, and health care operations
- An authorization is required for all other disclosures, except as required by law
- MGDPA does not differentiate between authorization and consent and requires a consent/authorization, with specific expiration date for **all** disclosures except as required by law

HIPAA vs. MGDPA (continued)

Lifeworks abides by the MGDPA rule as it is more stringent

Individual's Rights to Inspect or Copy

- HIPAA guidelines state that Lifeworks should act on a request to inspect or copy within 30 days
- MGDPA states that we must act on a request to inspect or copy within **10** days
- All requests should be submitted to Compliance Issues

HIPAA vs. MGDPA (continued)

Lifeworks abides by the MGDPA rule as it is more stringent

Request for Amendment

- HIPAA guidelines state that Lifeworks should respond to a request for amendment within 60 days
- MGDPA states that we must respond to a request for amendment within **30** days
- All requests need to be in writing and sent to Compliance Issues

Notice of Privacy Practices

- All persons served must be given a copy of the Notice of Privacy Practices (NPP) and sign the Release of Information and Acknowledgement of NPP
- All new persons served must receive NPP on or before the first day of services
- Both the person served and their legal representative, if they have one, must sign an acknowledgement stating they received a copy of the NPP
- Describes how the PHI of the person served may be used and disclosed by Lifeworks
- Details the persons served privacy rights regarding their PHI and how to exercise those rights
- Details the legal obligations of Lifeworks to protect PHI

Persons Served Privacy Rights

- Right to inspect and copy (access) their PHI
- Right to request restriction of uses/disclosures of their PHI
- Right to request alternative confidential communications from Lifeworks
- Right to request an amendment of their PHI
- Right to receive an accounting of certain disclosures of their PHI
- Right to obtain a paper copy of the Notice of Privacy Practices
- Right to file a complaint about violations of their privacy rights and/or Lifeworks privacy practices

Other Privacy Rule Requirements

- Minimum Necessary Standard
- Personnel Training
- Sanctions (Disciplinary Actions)
- Business Associate Agreements (BAA)
- New requirements as of September 23, 2013

Minimum Necessary

Too Much Information!

- **Key elements of the Privacy Rule**
  - Lifeworks Personnel with access to PHI have an obligation to limit that access and use to a minimum extent necessary to perform their duties and responsibilities
  - When requesting PHI, only request what is needed to accomplish the intended purpose of the request
  - When disclosing authorized PHI, only disclose the minimum amount to accomplish the intended purpose of the disclosure

Personnel Training

- Lifeworks must train all Personnel who access PHI on our Privacy Policies and procedures relating to PHI
- All new Personnel must receive the initial training within 1 week of their start date
- Annual training for all Lifeworks Personnel normally takes place in January each year
- **Personnel** means paid and unpaid staff (including employees and contractors), volunteers, student interns, and other persons who work for or on behalf of Lifeworks

Sanctions

- Lifeworks will apply disciplinary actions for any Personnel who violates the Privacy and Security Policies, procedures, or the state and federal privacy laws
- The sanctions are determined by the severity of each individual violation, potential violation, and breach of unsecured PHI
- Sanctions include disciplinary actions up to and possibly including termination of employment and possible reporting to law enforcement authorities

Penalties for Violating Privacy Laws

- The Office of Civil Rights and Department of Health and Human Services can impose penalties on individual Personnel, as well as on Lifeworks
- A person who knowingly obtains or discloses PHI in violation of the Privacy Rule may face a criminal penalty of up to $50,000 and up to one year imprisonment
- The toughest criminal penalties are for any person who **willingly** uses or discloses PHI (for personal gain) in violation of the Privacy Rule: up to $250,000 and 10 years imprisonment

Business Associate Agreements (BAA)

- Lifeworks must enter into a BAA with persons or agencies who provide services for Lifeworks and who access PHI in the course of those services
- BAA is a written contract stating that the Business Associate (BA) will comply with all HIPAA regulations and will appropriately safeguard and protect the security, confidentiality, and integrity of the PHI they receive from Lifeworks
- Lifeworks may be a BA of another agency when we provide services to them and access PHI in the process of those services (e.g. scanning or paper shredding services or projects)

HIPAA Breach Notification Rule

- As part of the HITECH Act, a new Breach Notification Rule went into effect September 2009
- **Breach: unauthorized acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule and such action compromises the security or privacy of the PHI**
- The Rule requires that Lifeworks notify individuals whose PHI was breached whenever that breach could pose a significant risk of financial, reputational, or other harm to the individual

HIPAA Breach Notification Rule (cont.)

Should YOU report a Breach or privacy violation?

- **Yes,** all Lifeworks Personnel have a responsibility to report **all suspected and actual violations**
- Notify someone within 24 hours of learning of the Breach or privacy violation:
  - send an email to Compliance Issues or
  - Notify Supervisor or
  - Open an IT Fresh Service ticket, or in an emergency, call the Lifeworks IT Service Desk at **651-365-3786**

Compliance Department is here to help!

Lifeworks Security Policies

Define safeguards to ensure the confidentiality, integrity, and security of ePHI

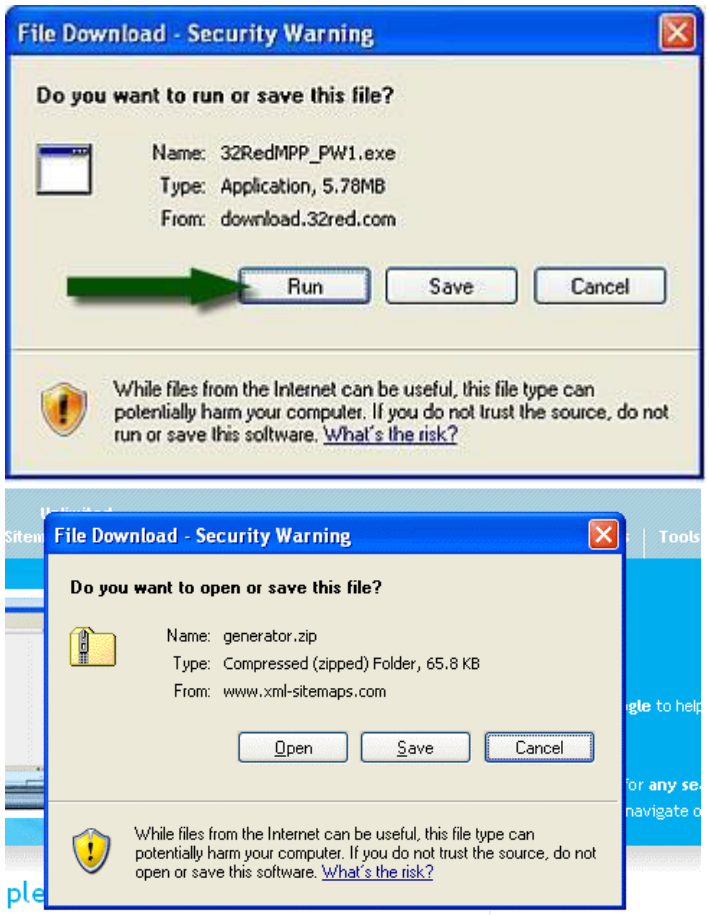
What is the **Security Rule**?

- The HIPAA **Security Rule** focuses on administrative, technical, and physical safeguards specifically as they relate to electronic PHI (ePHI)

- Protection of ePHI data from unauthorized access, whether external or internal, stored, or in transit, is essential to the HIPAA **Security Rule**

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

Safeguards: Malicious Software



Malicious Software

- Often installed by downloading software from the Internet
- Malicious emails attempt to install malware and spyware

Malicious Software Protection

- Virus protection/firewalls
- IT Acceptable Use Policy
- **Only IT is permitted to download and install software on Lifeworks devices**
- Open an IT Freshservice ticket to request software changes

Safeguards: Fax Documents


LifeWORKS
A nonprofit serving people with disabilities

CONFIDENTIAL FAX

DATE:

TO:

COMPANY:

FAX NUMBER:

FROM:

DIRECT NUMBER:

NUMBER OF PAGES (including this cover sheet):

NOTES/COMMENTS:

LifeWorks Services, Inc.
Administrative Office
2965 Lone Oak Drive
Suite 180
Eagan, MN 55121

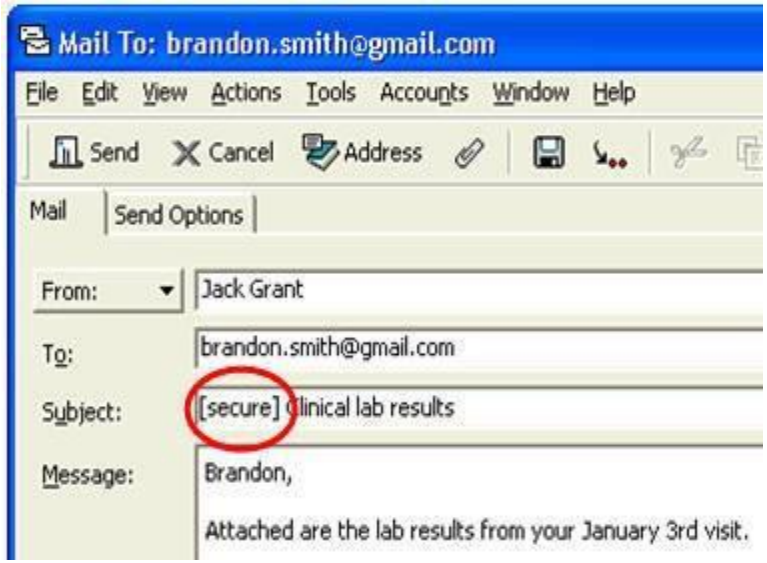
Phone: 651-454-2732
Fax: 651-454-2174

IMPORTANT: This facsimile transmission contains confidential information, some or all of which may be protected health information as defined by the federal Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule. This transmission is intended for the exclusive use of the individual or entity to whom it is addressed and may contain information that is proprietary, privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient (or an employee or agent responsible for delivering this facsimile transmission to the intended recipient), you are hereby notified that any disclosure, dissemination, distribution or copying of this information is strictly prohibited and may be subject to legal restriction or sanction. Please notify the sender by telephone (651-454-2732) to arrange the return or destruction of the information and all copies.

Fax Documents

- Always use a **Confidential Fax** cover sheet
- Pick up fax sheets in a timely manner to prevent loss or unauthorized access
- Store and shred fax sheets containing PHI appropriately

Safeguards: Emails



Email

- Confidentiality statement is automatically attached for emails to external parties
- Encryption for external emails: use [secure] in **subject** line
- Secure email procedures located in Document Templates -> Operations -> Information Technology -> Secure Email Guide
- **NEVER** put PHI in **subject** line

Safeguards: Computers

Computers

- Log out or lock screen when not using
- Displays in public areas should be turned in a way so that ePHI cannot be seen by others or a display privacy filter should be used
- No ePHI stored on the local hard drives or memory of laptops, desktops, tablets, or mobile phones

Mobile Devices

- All Lifeworks mobile devices that connect to the network or contain ePHI will be treated as computers
- **Personal** devices of Personnel are not allowed to connect (WiFi or otherwise) to the Lifeworks network or to contain ePHI of persons served

Safeguards: Computers (continued)

Computer Passwords

- Contain at least 12 characters
- Contain at least 3 of the 4 following character sets:
  - Uppercase letters
  - Lowercase letters (includes spaces)
  - Digits (0 - 9)
  - Special characters: !$%^&*()_+|~-=\`{}[]:";'<>?,/

Exception:
Lifeworks mobile phones and tablets must use the password IT assigns!

Safeguards: Security Incident Reporting

Security Incidents

- Virus, worm, other malicious attacks
- Network or system intrusions
- Unauthorized access to ePHI
- Loss or theft of Lifeworks computers, phones, tablets
- ePHI loss or unauthorized alteration

Reporting

- All users of ePHI must notify IT **immediately** of all security incidents affecting ePHI
  - For an emergency, call the Lifeworks IT Service Desk at **651-365-3786**
  - Open an IT Freshservice ticket
  - Notify Supervisor

Safeguards: Security Reminders

Logs and Monitoring

- IT will log and monitor computer activity (including emails) for potential security threats
- Lifeworks owns all email communications
- See also **Use of Equipment** and **Information Technology Acceptable Use Policy** in the handbook

Security Updates

- Communicated to Managers and Supervisors
- Posted on Lifeworks Today
- Posted on the IT Security page (under **Quick Links:**)
- Annual training

Safeguards: ePHI Security

Who is Responsible for ePHI Security?

- **YOU! YOU! YOU!**
- The greatest risk to the security of ePHI is human error and neglect
- The best defense against an internal or external breach is not technology but your security awareness
- **Your commitment to protecting ePHI is critical!**

Resources

Were do you find the policies?

- Privacy Policy, Security Policy, and Notice of Privacy Practices are located under Resources on the Lifeworks Today intranet website
- Privacy and Security Policies are Addendums to the Employee Handbook

Questions?

Contact Information

- Open an IT Freshservice ticket
- Email compliance isssues@lifeworks.org
- For an emergency, call the IT Service Desk Line at **651-365-3786**

Lifeworks Compliance and IT Departments