Legacy Mandatory Education Self-Study Module: HIPAA Information Security

HIPAA Security - What Are We Protecting?

HIPAA security guidelines are designed to guard **Electronic Protected Health Information (ePHI).** Inappropriately accessing or releasing this information is a HIPAA violation. It can violate a patient's privacy or affect a patient's care.

What is ePHI? *ePHI includes anything that can be used to identify a patient. For example, a patient's:*

- Name
- Date of Discharge
- Social Security Number
- Medical Record Number
- Phone Number
- Date of admission
- Date of birth
- Street Address, Zip Code, City, State
- Fax Number
- Email Address
- Date of Death (ages 90 and over)
- Account Number
- Health Plan Beneficiary Number
- Certificate / License Number
- License Plate Number
- Vehicle ID Number
- Photo Images *(full face)*
- Device ID or Serial Number
- Web Address ("uniform resource locator" or URL)
- Internet Protocol (IP) Address
- Fingerprints, Voiceprint, or Biometric ID
- *... and any other unique identifier*

HIPAA security covers all ePHI, whether it is stored on:

- Computers
- Tapes
- CDs
- Disks
- Thumb drives
- *Etc.*

...or sent electronically over the Internet or by email.

To protect ePHI, Legacy relies on:

1. **Monitoring technology,** to track system use
2. **Strong policies,** to prevent problems such as fraud and identity theft
3. And, most importantly, **our employees** to support Legacy's HIPAA security policies and report any concerns or suspected violations

System Monitoring

It is important to be aware that all communication on any of Legacy's computer or communication systems is subject to monitoring and review.

Monitoring systems can track:

- Anything written in or attached to an email
- All Internet activity (websites visited, times and durations, etc.)
- Access of patient medical records in E-Chart, Cerner Millennium, EPIC, etc.
- Data entry and modification
- Any failed login attempts

Important Note: *Monitored information can be reviewed at any time, and without notice, by Legacy management, Human Resources, or Information Services.*

Workstation, Laptop, Smart Phone, PDA, and Mobile Computing Device Use

These policies help us to balance the convenience of mobile devices with the need to protect our patient's ePHI:

Do	Don't
• Get approval from IS for any PDAs, smart phones, laptops, or thumb drives used for storing or accessing Legacy systems or ePHI.	• Bring non-LHS workstations, laptops, thumb drives, CDs/DVDs, etc. to work, connect them to the network, or use them to store or access LHS or ePHI data without prior approval from IS. • Install, remove, or change hardware or software without approval from IS. • Change configuration or security settings on an LHS or IS-approved device without approval from IS. • Leave a device or program open and unattended without enabling a password-protected screensaver or logging off the device.

Internet and Email

The Internet and email are great tools for research and communication, but they can be used in inappropriate ways. For example:

- Sending confidential information - including ePHI - to a third party without following LHS approved procedures
- Uploading or downloading software without prior authorization from IS
- Accessing objectionable materials not specifically related to job function
- Distributing copyrighted material, such as electronic documents, images, videos, sound files, etc., without permission
- Accessing blocked websites
- Using unapproved "chat" or instant messaging services
- Sending ePHI by email to any non-Legacy (lhs.org) email address without encryption, or without the IS-approved email encryption program. Contact IS with questions and to have the approved secure email software installed

Password Policies and Guidelines

Strong passwords are the first line of defense in protecting ePHI and our computer systems. These policies help us keep passwords from being "cracked":

Do	Don't

• Use strong passwords. *IS recommendations for creating a strong password are:*
  • Minimum of eight (8) alpha-numeric characters (a-z and 0-9) (*where systems allow*)
  • Not the same as any of the previous 5 passwords used
  • Not words found in a dictionary (English or foreign)
  • Not names, birth dates, SSNs, pet's names, etc.
  • Changed periodically (recommended every 90 days)
• Only use access specific to your job responsibilities
	• Share passwords with anyone (not even Help Desk, or system administrators). *Sharing your privileges with others is a violation of security policy, and may let them access more than they are allowed in order to do their job.*
	• Write passwords down (physically or in electronic files), or "sticky" them somewhere.

YOU are the key to Legacy's compliance with HIPAA security rules!

If you know about - or suspect - unauthorized activity on LHS computer systems or other electronic resources, you are responsible for reporting it to either the IS Help Desk, security official, or your supervisor.

Some examples of unauthorized activity are:

- Someone asking for your password and claiming to be from technical support
- A co-worker looking at a patient's medical record when they don't need to do so for their job
- An employee accessing his/her own medical records, or medical records of friends or family without proper approval
- Scanning admissions for friends or family
- Asking to borrow an ID badge
- Using someone else's password

If you have experienced - or suspect - a computer security attack or security violation, please notify the Information Security Group by contacting the Help Desk (x55888), or email information security directly at infosec@lhs.org

Some examples of security attacks or security violations to watch out for:

- Suspected computer viruses
- E-mail "phishing" (email claiming to be from an official person or organization, asking for a password or other sensitive information or ePHI)
- A "social engineering" attempt (an attempt to trick someone into giving sensitive or protected information)
- Password sharing
- A breach of physical security
- Disposal of ePHI by insecure means
- Unauthorized hardware or software use

Some examples of medical identity theft schemes to watch out for:

- A patient presenting with suspicious documents for identification
- A person (employee, patient, or other) that is inappropriately accessing/copying or taking medical records or health insurance information.

If you have witnessed or been alerted to a potential medical identity theft scheme, or have been notified by a patient that he or she is the victim of identity theft, please notify Legacy's Compliance Line: 1-800-820-7478.

Additional Resources

For more information on Legacy's information security policies, see the following policy documents:

- 700-24: Electronic Systems and Communications
- 700-26: Electronic Information Security
- Legacy's Identity Theft Prevention and Detection Program *(policy document coming soon)*
- Legacy's Compliance Line **1-800-820-7478**
- Legacy's HIPAA Hotline **503-413-4495**

Anyone using Legacy electronic information systems needs to be familiar with these resources.

Contact Us

Legacy's Security Official is Tony Wente, Dir. of Technical Operations. Email the Information Security Group at infosec@lhs.org to report any suspected security incidents or with questions.