Information Technology and Services

Information Security Awareness Training

LIFEPOINT HOSPITALS®

WHY?

LIFEPOINT HOSPITALS

- **Regulations**
  - HIPAA Privacy & Security Acts
  - ARRA / HITECH Act (tightening HIPAA regulations)
  - Penalties & consequences for non-compliance
- **Systems and data are essential to LifePoint Hospitals' ability to provide services**
  - LPNT requires a safe and secure computing environment
  - Confidential data must be protected from unauthorized access
  - Minimize disruptions to systems and network infrastructure
- **We live in a new electronic environment**
  - Threats: identity fraud, theft, hacking, denial of service, cyber criminals, etc.
  - Changing attitudes towards technology leads to a relaxed sense of danger

Penalties

LIFEPOINT HOSPITALS

- Loss of access privileges
- Disciplinary action - loss of system access or user privileges could mean loss of job if you need the system to do your job.
- Termination of employment (or business relationship)
- Criminal and civil prosecution under state and federal law
- Monetary fines – These can be leveraged against individuals not just the facility / employer you work for.
  - Civil – Up to $50,000 per violation not to exceed $1.5 million per year
  - Criminal - $250,000 Per violation
- Imprisonment – Criminal only – up to 10 years in prison

General Security Principles

LIFEPOINT HOSPITALS

- Each user is **accountable** for their conduct while accessing company electronic assets.

- Use of electronic resources may be monitored or recorded for security reasons and for assessing compliance with company policies and procedures. *There should be* ***no expectation of privacy.***

- Your obligation to uphold these standards and confidentiality of company information **continues *even after* termination** of your employment or after your relationship with the company ceases.

Access

LIFEPOINT HOSPITALS

- **Restrict physical access to confidential systems, data, or equipment**
  - Locks, clean desk policy, badges, card swipe, security cameras
  - Do not defeat security mechanisms (ex: prop open a door)
- **User IDs and Passwords**
  - Never share or divulge to ANYONE
  - Lock computer when unattended (Ctrl-Alt-Del)
  - Request account to be disabled when on leave of absence or non-use
  - Passwords should not be written on post it notes and posted under keyboards or other devices
- **Least Privilege**
  - Department managers are responsible for requesting appropriate access
  - Deny access (privileges) if not absolutely required for your job
  - Access changes when job duties change
  - Managers must review access of staff periodically
- **System Activity Review**
  - User Audits are routinely performed
  - Be aware how you access and use information on our systems are monitored
- **Termination Procedures**
  - When employment ends department managers must request access to be disabled immediately

Social Engineering

LIFEPOINT HOSPITALS

The act of using deception to gain unauthorized access

Examples:

- Impersonation – of an employee, computer support person, administrator, trusted source, etc.
- Phishing – getting you to divulge information (user ID, password, personal identifiers, company information, etc.) you shouldn't - via email, the Web, or in person
- Capitalizing on human carelessness (ex: dumpster diving) , playing on your sympathy, using intimidation

Don't be a puppet!

Do Not . . .

LIFEPOINT HOSPITALS

- ...store PHI on USB drives or local hard drive if not encrypted
- ...store PHI on CDs or DVDs if not encrypted
- ...store PHI on public network share drives
- ... leave PHI unattended that can be accessed through the hardware or media
- ...install/copy software; use only authorized, licensed, LPNT-provided software
- ...remove, relocate, or dispose of electronic equipment
- ...defeat security mechanisms (physical or electronic)
- ...use LPNT systems for outside business or personal gain

Never…

- …Connect wireless access point devices to any company network
- …Store sensitive business data on un-authorized Wi-Fi network storage devices

Do . . .

LIFEPOINT HOSPITALS

- Utilize software encryption when storing sensitive business information on media
- Dispose of confidential paper material in secure shred-it bins
- Lock your computer (Ctrl-Alt-Del) when unattended
- Use automatic system log-off's controls when available
- Store data to approved network drive, not local hard drive
- Remove all PHI from any media before it is made available for re-use
- Return all media and equipment in good condition when you leave the company
- Notify your manager, FISO, Privacy Officer and/or IT Service Desk to voice security concerns/questions
- Report any witnessed or suspected suspicious activity or use of systems to your FISO

Email

LIFEPOINT HOSPITALS

- Not private! May be monitored.
  - Deleted messages are still traceable.
  - Do not send broadcast emails, chain letters, etc.
- Never use in email:
  - LPNT UserID's and Passwords
  - Non-Encrypted PHI (protected health information)
  - Individual identifiers, such as social security number
  - financial information, such as credit card or billing information

Electronic Communications

LIFEPOINT HOSPITALS

- Never use inappropriate language or discuss inappropriate or offensive topics
  - Never use racial, religious, political, threatening, or sexual overtones
- Do not download or circulate music files or copyrighted materials
- Do not photograph company materials or employees without permission.
- Do not photograph patients without a valid, HIPAA compliant patient authorization unless it is required as part of your job.
- If you are emailing PHI or sensitive data to someone *outside* of LifePoint, or you are uncertain whether the recipient's email address is within LifePoint, you must encrypt the email or file(s). When in doubt, encrypt

Email Subject Line

[encrypt] (with brackets) somewhere in the Subject line.

For additional Guidance see Information Security Guidance Documents on "SharePoint"

Responsibility

LIFEPOINT HOSPITALS

- The Facility Information Security Official (FISO) is responsible for the local security compliance program.

- HIPAA-compliance documents, policies and procedures must be maintained for 6 years from the date of creation or the date when it last was in effect, whichever is later.

- The retention of maintenance records to document repairs and modification to physical components related to security are included in this documentation requirement.

Emergency Preparedness

LIFEPOINT HOSPITALS

- Not just IT! It is **everyone's responsibility**!
- Contact lists / call trees for your department
- Ensure security and confidentiality of PHI is maintained, even in a disaster
- Know and practice **downtime procedures** (how to do your job even if the computer systems are down)
- Create and test a **disaster plan** for your area

Security Incidents

LIFEPOINT HOSPITALS

Examples:

- Lost or stolen laptop or Blackberry
- Password that has been compromised
- Loss of data or confidentiality (breach)
- Inappropriate use or destruction of company data or electronic resources
- Threat of a crime (ex: harassing email)
- Cyber attack, malicious code (virus), etc.
- Defeating a security mechanism (ex: propping open a locked door)
- Non-compliance with any security-related policy, standard or procedure

Incident Reporting

LIFEPOINT HOSPITALS

- For disclosures of PHI or privacy breaches, contact the Facility Privacy Officer and the Facility Information Security Official.
- Incident Reporting is an obligation, this should be done without fear of retaliation, and may be made anonymously.
- LifePoint Ethics & Compliance Hotline. 1-877-508-LIFE (5433)
- For additional Guidance see HIPAA.GEN.007 Protected Health Information Incident Response.

More Information

LIFEPOINT HOSPITALS

Read all IS Security Policies & Standards posted on the LifePoint Hospitals Intranet

http://sharepoint.lpnt.corpad.net/sites/it/infosec

We are all accountable for understanding and abiding by all policies and standards.