CONEMAUGH SCHOOL OF NURSING & ALLIED HEALTH PROGRAMS

Cybersecurity Policy Manual

2024-2025

Table of Contents

Reviewed 8/8/2024

Conemaugh School of Nursing and Allied Health Schools

Data Security Requirements for Higher Education

As a Title IV Postsecondary Institution (PSI), Conemaugh School of Nursing & Allied Health is considered a financial institution per the Gramm-Leach-Bliley Act (GLBA, 2002). Per the Federal Student Aid Program Participation Agreement and the Student Aid Internet Gateway Agreement, a PSI must have GLBA safeguards in place. PSIs without GLBA safeguards may be found administratively incapable (unable to properly administer Title IV funds).

Conemaugh School of Nursing & Allied Health has developed the following data security program, along with Conemaugh Memorial Medical Center. This security program is reviewed annually by Conemaugh's Management Information Systems Department and the Associate Director of the Conemaugh School of Nursing & Allied Health Programs. Reviewing the policies annually allows the school to identify foreseeable internal and external risks to data security and to evaluate and adjust the program accordingly. Employees of the School are trained and educated yearly during Faculty Education Day and during mandatory annual online training.

For questions regarding the information contained within this policy please contact:

Conemaugh Management Information Security Department: 814-534-9195

James Ahacic MSN, RN, Interim Director, Conemaugh School of Nursing & Allied Health Programs: 814-534-9480

What is a Breach?

Per GLBA, PSIs must protect against any unauthorized disclosure, misuse, alteration, destruction, or other compromise of information, such as unauthorized access. The Department of Education and Federal Student Aid considers each of these a breach. Each PSI must have in place administrative, technical, and physical safeguards which

- ensure the security and confidentiality of customer information,
- protect against any anticipated threats or hazards to the security or integrity of such records, and
- protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Reporting Breaches to the Department of Education

The Student Aid Internet Gateway Agreement requires that as a condition of continued participation in the federal student aid programs, PSIs report actual data breaches, as well as suspected data breaches. Title IV PSIs must report on the day that a data breach is detected or even suspected. The U.S. Department of Education (the Department) has the authority to fine institutions—up to $54,789 per violation per 34 C.F.R. § 36.2—that do not comply with the requirement to self-report data breaches.

To report a breach, the school must email cpssaig@ed.gov . The email should include the:

- date of the breach (known or suspected),
- impact of the breach (number of records, number of students, etc.),
- method of the breach (hack, accidental disclosure, etc.),
- information security program point of contact (email address and phone number are required), • remediation status (complete, in-process, etc. with detail), and
- next steps (as needed).

If unable to email, School's should call the Department's security operations center (EDSOC) at 202-245-6550 to report the data listed above. EDSOC operates 24 hours a day, seven days per week. If both previous breach-reporting methods fail, School's should call or email Tiina Rodrigue at 202-377-3887 or tiina.rodrigue@ed.gov. After the initial report, breach status updates can be emailed directly to Tiina.

Conemaugh Information Security (Cybersecurity) Policies

I. Overall Policy Statement:

The purpose of this policy is to provide a security framework that will ensure the protection of School Information from unauthorized access, loss or damage while supporting the open, information-sharing needs of our academic culture. School Information may be verbal, digital, and/or hardcopy, individually controlled or shared, stand-alone or networked, used for administration, research, teaching, or other purposes. Standards and procedures related to this Information Security Policy will be developed and published separately. Failure to comply with the following policies may subject you to disciplinary action. All LifePoint Health Policies can be located on the Intranet, Policy Stat system.

II. Who Is Affected

The following policies not only apply to Conemaugh Memorial Medical Center employees but to all School faculty and staff, as well as to students acting on behalf of the Conemaugh School of Nursing and Allied Health through service on school bodies such as councils and committees. The policies also apply to all other individuals and entities granted use of School Information, including, but not limited to, contractors, temporary employees, and volunteers.

III. Definitions

Authorization – the function of establishing an individual's privilege levels to access and/or handle information.

Availability – ensuring that information is ready and suitable for use.

Confidentiality – ensuring that information is kept in strict privacy.

Integrity – ensuring the accuracy, completeness, and consistency of information.

Unauthorized access – looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and legitimate business need.

School Information – information that Conemaugh collects, possesses, or has access to, regardless of its source. This includes information contained in hard copy documents or other media, communicated over voice or data networks, or exchanged in conversation.

LifePoint Health Policies

1. Data Protection on Electronic Media

SCOPE:

This policy applies to all subsidiaries and affiliates of LifePoint Health (the "Company") and all employees of any of them.

PURPOSE:

To establish requirements and responsibility for protecting electronic Company Confidential and Restricted information on electronic media.

POLICY:

1. All Facilities and LifePoint Health departments are responsible for ensuring compliance with Company Policies, Standards, and procedures to reduce the risk of loss or disclosure of Confidential and Restricted information stored on electronic media.
2. In the event of inappropriate information disclosure caused by a failure to comply with Company Policies, Standards, and procedures, any cost associated with breach notification or other related activities may be allocated to the Facility or LifePoint Health department responsible.
3. Workforce members using electronic media must protect the media and any information stored on it pursuant to applicable Company Policies and Standards. In the event of inappropriate information disclosure caused by a failure of a workforce member to comply with Company Policies, Standards, and procedures, appropriate sanctions will be enforced per HIPAA.GEN.003, HIPAA Complaint Process and Disciplinary Guidelines Policy.

DEFINITIONS:

Confidential and Restricted Information: Confidential and Restricted Information includes data that, if disclosed, could result in damage to the company, an individual, or other stakeholders. It can include passwords, social security numbers, protected health information (PHI), financial data such as bad debt records, and our employees' human resources files. See the Electronic Data Classification Standard for more information.

Media*:* Any electronic asset, regardless of ownership, that has the potential to store, process, or transmit Company information.
Portable Device*:* Electronic media that is designed for mobility, such as a laptop computer, Tablet, Camera, or Smart Phone.
Removable Media*:* Electronic media that can be easily removed from a system, such as a USB ("thumb") drive, memory card, CD/DVD, video tape, backup tape, "hot swap" server drive, or an external hard drive.

Workforce Members: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a facility, is under the direct control of such facility, whether or not they are paid by the facility.

PROCEDURE:

A. **Data Protection: Facility Responsibilities**
   1. Facilities and LifePoint Health departments are responsible for educating users of electronic media regarding the risks of loss or disclosure of Confidential and Restricted information stored on such devices. Education must occur at the time the media is assigned to the workforce member. In addition, facilities must provide education anytime a workforce member fails to comply with relevant Company Policies, Standards, or procedures.
   2. Facilities and LifePoint Health departments must communicate and enforce appropriate sanctions for workforce members who fail to follow appropriate Company Policies, Standards, and procedures designed to reduce the risk of loss or disclosure of Confidential and Restricted information stored on media as outlined in the HIPAA.GEN.003, HIPAA Complaint Process and Disciplinary Guidelines Policy.
   3. Facilities and LifePoint Health departments must implement technical and physical safeguards to protect Confidential and Restricted information stored on media in the event the device is lost or stolen. Implementation of these safeguards must meet the requirements defined by the relevant Company Policies, Standards, and procedures.

B. **Data Protection: Workforce Member Responsibilities**
   1. Workforce members must only store Company information on electronic media which their facility IT or Health Informatics and Technology Services (HITS) team within the LifePoint Health Support Center (HSC) has authorized them to use, and only for the authorized purposes.
   2. Workforce members may store Confidential or Restricted data on portable and removable media only when, and for so long as, it is required by their job role or function.
   3. Workforce members who use portable and/or removable media must physically secure or maintain control of the media at all times.
   4. Workforce members must apply appropriate technical safeguards to protect any Confidential or Restricted information transferred to portable devices or removable media. Implementation of these safeguards must meet the requirements defined by the relevant Company Policies, Standards, and procedures. See the Media Controls Standard for more information.

C. **Reporting a Loss or Theft**
   1. Workforce members must immediately inform the designated Facility Ethics and Compliance Officer (ECO), Facility Privacy Officer (FPO), or the Facility Information Security Officer (FISO) of any suspected loss of electronic media potentially containing Confidential/Restricted information, or potential disclosure of any Confidential/Restricted information stored on electronic media. Alternatively, reports may be made anonymously in accordance with the Company Code of Conduct.
   2. Once notified of a suspected incident, ECOs, FPOs and FISOs must immediately report the suspected incident in accordance with LPNT.IS.SEC.010, Protected Information Incident Response Policy.
   3. Facilities and LifePoint Health departments must ensure any workforce members involved with the suspected loss or disclosure of any Confidential/Restricted information stored on electronic media are available to the Company Core Event Response Team "CERT" and complete any required incident response tasks in a timely manner.

2. Acceptable Use of Technology Resources

STATEMENT OF POLICY

It is the policy of Conemaugh Health System (CHS) to establish requirements for the use of computing technologies. Such requirements are necessary to ensure compliance with Federal copyright and Privacy laws and other applicable laws and regulations and to protect the system from the risk of computer viruses, hackers, and other similar threats. This policy applies to all authorized users, including but not limited to physicians, employees, and contractors.

Access to electronic information and use of computing technologies are provided to authorized users and shall be used as business tools for appropriate internal and external business use, and for routine performance of job-related duties.

Authorized users whose access or use of information is deemed unacceptable may be in violation of State/Federal laws and/or CHS policies (Medical Staff Bylaws, Performance Improvement Policy, and Information Security and Privacy Sanctions Policy) and subject to appropriate disciplinary action up to and including termination of employment or contractual relationship and/or pursuit of civil/criminal action or other legal remedy.

For more information on information security at CHS, refer to the Information Security Program policy, and the Information Security and Privacy Sanctions policy.

SCOPE OF POLICY / DEFINITIONS

1. This policy applies to all workforce members' authorized use of all workstations and information resources.
2. Information Resource - any system, database or file containing information specific to CHS, including but not limited to electronic Protected Health Information.
3. Workstation - any electronic computing device, i.e., desktop, laptop, notebook, wireless device, smartphone, diagnostic equipment, etc.
4. Shared workstation - an electronic computing device regularly used by multiple users, i.e., desktop computers and wireless laptops on nursing units which are used by nurses, unit clerks, physicians and ancillary staff; diagnostic equipment used by multiple ancillary staff members within the ancillary department, etc. Workstations that are not 'shared' are assigned to one workforce member and are not used by others on a regular basis.
5. Remote Access - any connection to CHS's network and/or other applications from an off-site location such as a user's home, Internet hot-spot, etc.
6. Mobile Device - any device capable of storing information and/or connecting to the Conemaugh network without physical cables, including but not limited to, smartphone, cell phone, tablet computer, etc.
7. Portable Storage Media – any data storage medium that can be readily removed from the host computer. Examples of portable storage media include CD's, flash drives, backup tapes, external hard drives, etc.
8. Electronic Protected Health Information (ePHI) – any electronic information that could enable someone to determine the individual's identity (name, phone number, social security number, etc.) and relates to at least one of the following:
    - The individual's past, present or future physical or mental health

- The provision of health care to the individual
- Past, present, or future payment for health care

Accountability – General Requirements

1. Users must adhere to the CHS Code of Conduct and behave in an ethical, proficient, informed, and trustworthy manner.
2. CHS provides computing and information resources, including Internet access, to authorized users and provides Information Security training and other security resources to them.
3. All users granted authorization to utilize computing resources must sign a legally binding agreement on appropriate use of those resources.
4. All new workforce members must receive CHS Information Security Basic training as part of their orientation.
5. User IDs and passwords help maintain individual accountability for computing resource usage. **Any authorized user who obtains a password or login ID from CHS must keep that password confidential and responsibly select and manage passwords**. Users are prohibited from sharing user IDs or passwords obtained for access to Internet sites, email, internal databases, and information systems, etc.
6. CHS reserves the right to monitor all hospital electronic records, including e-mail messages, files, Internet sites and electronic record access. **Authorized users utilizing CHS computing facilities should have no expectation that their Internet use, e-mail messages, or other usage of CHS' information are private**. Anything that is created, sent, received, or stored on CHS' computer network is the property of CHS and, therefore, subject to investigation, review, and search by designated, authorized personnel without prior notice, either periodically as part of CHS standard information security audit procedures or as a result of a security incident.
7. CHS applies automatic antivirus and security updates to workstations on its network. Disabling or tampering with such software, the purposeful introduction of viruses, or malicious tampering with any computer system is prohibited.
8. Hardware and software installations are to be performed only by approved I.S. personnel. Workforce members, including vendors and contractors, are prohibited from installing hardware and components on any workstation or the CHS network without prior MIS approval.
9. Inappropriate use of CHS computing resources will not be tolerated. Excessive personal use of the computers during scheduled work hours is not permitted. The installation or downloading of executables/programs is not permitted for non-work associated use (including installing copyrighted software). Playing computer games is prohibited. Interaction on social media Internet sites such as Facebook and Google+ is prohibited without prior management approval.
10. All users are required to log out of (or otherwise make inaccessible, i.e., by locking the workstation) all applications or networks containing sensitive information prior to leaving their workstation.
11. CHS may remove or deactivate any user's privileges, including but not limited to, user access accounts and access to secured areas, when necessary to preserve the integrity, confidentiality and availability of its facilities, user services, and data.
12. Users must use only systems, software, and data for which they are authorized.
13. Users are to report observed security incidents, or any incidents of suspected fraud, waste, or misuse of CHS systems to appropriate individuals.
14. Users must protect confidential and/or sensitive information from disclosure.

15. Removal of computers or computer equipment from CHS premises is prohibited unless authorized in accordance with CHS property management procedures.
16. Individuals shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without prior permission. The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third party. Individuals must exercise caution and care when transferring such material in any form. In addition, all printed outputs should be removed immediately from the printer and stored in an appropriate location.

Physical Requirements

1. Workstations should be positioned such that they are facing away from public view. If the physical location of the workstation limits the ability to hide it from public view, users are to take additional actions such as using privacy filters and minimizing display windows, logging out of applications, or invoking screensavers before moving away from workstations.
2. All users are required to log out of (or otherwise make inaccessible, i.e., by locking the workstation) all applications or networks containing sensitive information prior to leaving their workstation.
3. Whenever possible, all files must be saved to network drives. If portable storage media must be used because the computer is not connected to the network or to move files between computers, the user must request an encrypted USB Drive from MIS. MIS will review the request and will assign a password-encrypted USB drive to the user if approved. Users are not to use any other form of portable storage media for off-line data storage and must return the encrypted drive to MIS when no longer required. All data saved to these devices should be transferred to a CHS network drive as soon as possible and then deleted from the USB Drive.
4. Computing equipment and media, including but not limited to workstations, monitors, keyboards, smartphones, portable storage media, must be disposed of properly.
    - Portable storage media must be disposed of in accordance with document destruction procedures in the secure shredding bins provided to departments. Portable storage media in an envelope separated from paper in bin.
    - All other computing equipment and media must be returned to MIS for proper data destruction and disposal.
5. Printers and fax machines should never be placed in public areas. Users should ensure that printed or faxed documents are retrieved from printers or fax machines promptly and placed in a secured location.

Internet and E-Mail Use Requirements

1. Individuals using CHS Internet accounts are acting as representatives of the organization and should act accordingly so as not to damage the reputation of the organization. An Internet user can be held accountable for any breaches of security or confidentiality. Examples of Internet and e-mail activity that are unacceptable , but are not limited to:
    - Posting confidential CHS information or ePHI to the Internet. The Internet does not guarantee the privacy and confidentiality of such protected health information, except where duly noted (such as a secure messaging connection)
    - The viewing or transmission of offensive or pornographic materials

- Sending racially or sexually offensive images. This includes accessing sites containing sexually explicit content that may constitute sexual harassment or be considered discriminatory, obscene, or derogatory.
- Making slanderous remarks or defamation of character
- Using CHS computers for recreational games or social media interaction
- Using CHS computers to download images, videos, MP3s or establish real-time audio/video streams for personal use. Uploading of any CHS licensed software owned or licensed by CHS.
- Excessive Internet access that adversely affects the network or job performance
- Sending/Forwarding "Chain Letters" through electronic mail
- Running a personal business with CHS resources; this includes performing personal activities for commercial gain
- Participation in any illegal activity
- Unless otherwise noted, all software and information on the Internet should be considered copyrighted work. Therefore, individuals are prohibited from downloading software and/or distributing downloaded information without express permission from the copyright holder.
- Any activity deemed unacceptable based on organizational or departmental policy

2. Files that are downloaded from the Internet for direct business use must be scanned with virus detection software before installation or execution. Contact the MIS Help Desk so that all appropriate precautions can be taken to detect a virus and, if necessary, to prevent its spread.
3. Social media interaction of any form is prohibited unless work related and approved by the individual's manager - refer to Social Media Policy for further information.
4. E-mail messages will be filtered to prevent incoming spam. Certain attachment types will be prevented from being sent or received to avoid the possible spread of viruses or other malicious code, for example: executables, screen savers, etc.
5. Automatic forwarding to an e-mail address outside of the CHS network is prohibited to avoid inadvertent transmission of sensitive information.
6. Confidential or sensitive information (including ePHI) should only be sent via e-mail when necessary, and then only in accordance with approved "secure mail" procedures as published in the Information Security Manual. Refer to Electronic Protected Health Information (ePHI) Requirements section for further information.
7. All e-mail messages addressed to locations outside of the Conemaugh.org network should have a confidentiality disclaimer embedded into the message.
8. Access to Personal Email Accounts from any Conemaugh-owned computer is not permitted. This includes access to any web-based personal email account such like Gmail, Hotmail, Yahoo, Atlantic Broadband, Comcast, etc. Furthermore, access to these email accounts from a Conemaugh-owned computer is prohibited even when the computer is not connected to the Conemaugh network (example – Conemaugh laptop connected to a home network, a hotel internet, guest network, etc.). This restriction applies only to Conemaugh-owned computers and not personal devices such as smartphones, tablets, etc.

Password Management Requirements

1. Each user must sign the CHS Confidentiality and Security Agreement before being provided access to CHS Information Technology resources. The agreement defines requirements which must be adhered to by all users. Users who do not abide by these requirements are subject to disciplinary action in accordance with the Information Security and Privacy Sanctions Policy.

2. User account information should be safeguarded as confidential information. Workforce members are not permitted to keep an unsecured written record of passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access location if in hardcopy form, or in an encrypted file if in electronic form.
3. When a user forgets their password and requires a new one, the appropriate system administrator providing the new password must ensure the identity of the user requesting the new/reset password. Such confirmation can be accomplished by voice or facial recognition, checking the CHS-provided photo identification, or by recognition of the manager requesting a password reset for one of their employees. Passwords will not be transmitted electronically over the Internet or through e-mail.
4. Each authorized user will have a unique user id/password for each application and their network access unless the application has additional security at the function level.
5. Where possible, applications are to enforce password security policies in accordance with the following guidelines. In cases where these guidelines cannot be system-enforced, users are required to follow these guidelines via manual interaction with application security settings:
    - Passwords must be a minimum character's length as defined by MIS.
    - Passwords must be changed immediately if it is suspected that the password has been compromised.
    - Passwords must not be the same as the User ID.
    - Passwords must not be based on well-known or easily accessible personal information (i.e., Social Security Number, birth date, child's name, pet's name, etc.) or common word such as "Conemaugh," etc.

Remote Access Requirements

1. Workforce members requiring remote access must first justify a business purpose that outlines why the access is required and what level of service the employee needs . Application forms must be approved and signed by the employee's manager, supervisor, or director before submission to MIS.
2. All remote access connections will be centrally managed by MIS and will utilize encryption and strong authentication measures.
3. Unless approved in advance by MIS management, no user is permitted to install any form or "remote control" software that enables them to access a CHS computer remotely. No CHS corporate information or ePHI of any kind is permitted to be stored locally on a user's personally owned computer desktop, C drive, or Portable Storage Media (ex. USB Drive). Additionally, Internet-hosted storage of any CHS corporate or ePHI information is forbidden without prior MIS approval. All information must be stored on a CHS network drive. Anyone who does not fully understand this requirement is strongly advised to contact their direct supervisor or MIS Help Desk for assistance. Individuals may be subject to civil and criminal prosecution for violating HIPAA Privacy and Security Rules regarding the protection of e-PHI.
4. The remote access device must have current firewall protection, anti-virus protection, and all current operating system security patches installed.
5. Workforce members will make no modifications of any kind to the remote access connection without the express approval of MIS. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware, or security configurations, etc.
6. Unless application requirements require otherwise, remote access sessions will time out after a minimum of 20 minutes of inactivity and will terminate after 4 hours of continuous connection.

7. Vendor requests for remote access must be accompanied by a signed Vendor/Contractor Data Security and CHS Confidentiality Agreement from the vendor and must be submitted and approved by the department manager/director. If the vendor's remote access will grant them access to electronic Protected Health Information and they are classified as a Business Associate, a signed Business Associate Addendum is also required.

Mobile Device Requirements (Smartphones, Tablet Computers, etc.)

1. Workforce members must take appropriate measures to prevent unauthorized access to confidential information stored on or accessed by a mobile device, including but not limited to the following:
   - log off remote connections and applications when not in use to prevent unauthorized access.
   - never leave the device unattended without physically securing it.
2. Loss or theft of portable devices used to access the CHS network must report the loss immediately to MIS regardless of whether or not the device is owned by CHS.
3. No CHS corporate data or ePHI is to be stored on a mobile device.
4. Mobile devices that access the CHS network should be configured with password access controls and data encryption.
5. Access to the CHS network via mobile devices that have had internal controls bypassed (i.e., Jailbroken) is prohibited.

Wireless Access Requirements

1. Users are not permitted to connect to the corporate encrypted CHS wireless network via personally owned devices. Such access is permitted only via the separate open-access wireless network that CHS operates for patients and guests.
2. MIS reserves the right to deny wireless network access without notice for any user and/or device.

Electronic Protected Health Information (ePHI) Requirements:

The following requirements pertain specifically to ePHI data management safeguards. The requirements are intended to support CHS efforts to protect patient information and comply with federal HIPAA regulations. Further information regarding HIPAA and confidentiality/privacy protection can be found in the "HIPAA Plan" policy located in the Organizational Policy manual.

1. ePHI is to be saved ONLY to network drives or in CHS applications specifically designed for ePHI storage whenever possible. Storing ePHI on a local hard drive or on a Portable Storage Media is prohibited unless approved full disk encryption is in place on that device. MIS is the only CHS entity permitted to configure a device with full disk encryption.
2. Storing ePHI on any Internet site such as Dropbox, Google Drive, Microsoft SkyDrive, Sharefile, etc. is strictly prohibited unless specifically approved by MIS for that purpose.
3. ePHI transmitted outside CHS must either first be encrypted via an MIS approved file encryption method or it must be encrypted during transmission. Once encrypted, files can be transmitted by common carrier. Transmission of unencrypted files must follow requirement #3.
4. HIPAA laws mandate that unencrypted ePHI can only be transmitted via a secure, encrypted communication method. The following are considered secure methods of communication:
   - Email containing ePHI to an external (non-Conemaugh.org) recipient sent via secure mail see instructions under Intranet/MIS Department)
   - Note - email containing ePHI transmitted to a Conemaugh.org recipient does not require being sent via secure mail.

- Secure FTP
- SSL Internet connection (i.e., https)
- VPN connection
- CHS Courrier – for physical transmission of Portable Storage Media
- Doc Halo (Conemaugh's approved secure texting application)

The following communication methods are not encrypted and **not** permitted for use in transmitting ePHI unless the ePHI has already been encrypted:

1. Text messages via any method other than Doc Halo
2. Instant messages
3. Unencrypted files or messages emailed to non-Conemaugh recipient
4. Any Internet-based communications (example – social media sites such as Twitter, Facebook, etc.) unless secured via SSL

Other Requirements

The following actions are prohibited at all times. Violations will be subject to the Information Security Sanctions Policy.

1. Accessing the Data/Telecom network with a diagnostic or testing tool such as a protocol analyzer intended to monitor, decode, or filter packets of information.
2. Entering a designated Telecom Closet or Data/Telecom Network equipment room without written authorization.
3. Attempting to physically or logically reconfigure, move, or disengage a Data/Telecom Network component.
4. Installing computer services on the Data/Telecom Network that increase CHS's vulnerability to denial-of-service attacks, viruses, or similar problems.
5. Install/uninstall, reverse engineer, decompile, disassemble, or modify any software or files on any CHS system/network without express consent of the Information Systems Department.

RESPONSIBILITY

Management Information Systems and Corporate Compliance are responsible for implementation of this policy and for on-going monitoring of compliance with its provisions. Corporate Compliance will also audit usage logs and other system reports to assure compliance to this and related policies. This policy will be enforced using the procedures outlined in the Information Security and Privacy Sanctions Policy.

3. Identity Theft Prevention Policy

STATEMENT OF POLICY

It is the policy of Conemaugh Health System (CHS) to comply with all federal and state laws and regulations in conducting business operations. The Federal Trade Commission (FTC) has issued regulations (the Red Flags Rules) that require financial institutions and creditors to develop and implement written identity theft prevention programs. These regulations were the product of the Fair and Accurate Credit Transactions (FACT) Act of 2003, which amended the Fair Credit Reporting Act (FCRA). The final rules were published in November 2007. Identity theft prevention programs must provide for the identification, detection, and response to patterns or specific activities--known as "red flags"--that could indicate identity theft.

PURPOSE

CHS and its affiliates strive to prevent the intentional or inadvertent misuse of patient names, identities, and medical records; to report criminal activity relating to identity theft and theft of services to appropriate authorities; and to take steps to correct and/or prevent further harm to any person whose name or other identifying information is used unlawfully or inappropriately.

The purpose of this policy is to comply with the FACT Act by ensuring that we have a process in place to identify and detect red flags and prevent and mitigate the harm from identity theft. Additionally, we must continuously update the identity theft prevention program as changes in methods of identity theft evolve, as well as changes in means to detect identity theft become available.

DEFINITIONS

A **creditor** is an organization or individual that regularly extends, renews, or continues credit.

Credit is the right granted by a creditor to a debtor to defer payment. CHS permits our patients to defer payments for medical services provided, so credit results.

An **account** is a continuous relationship between a service provider, for example, and a customer.

A **covered account** is (1) a consumer account that is designed to permit multiple payments; or (2) a business purpose account for which there is a reasonably foreseeable risk of identity theft. CHS has covered accounts with our patients that fit both of these categories.

Identity theft is fraudulently using the identifying information of another person, for example, to open a credit card account, establish phone service in the victim's name, acquire a driver's license in the victim's name, and even provide the victim's name to police during an arrest.

Red flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. The Red Flags Rule picks up where data security leaves off. Data security practices make it harder for crooks to get access to the personal information they use to open or access accounts. Red flags are the alerts to be on the lookout for that indicate fraud may be occurring (sort of a head's up).

Medical identity theft occurs when someone uses a person's name, and sometimes other parts of their identity, such as insurance information, without the person's knowledge or consent. The individual then obtains medical services or goods or uses the victim's identity to make false claims for medical services or goods. The result can be erroneous entries into the victim's existing medical records and/or could lead to fictitious medical records in the victim's name. The victims of medical identity theft have all the same problems of identity theft victims; however, the victim also has to worry that his medical records have been altered and may be confused with that of the thief.

PROCEDURE

I. Identification of Covered Accounts

A. Accounts that would likely contain sufficient information that, if stolen, could lead to identity theft would include the following:

1. Patient accounts
2. Billing records
3. Leases to third parties of office space, equipment, or personnel

4. Any account that involves multiple payments, or those for which there is a reasonably foreseeable risk of identity theft (including financial, operational, compliance, reputation, or litigation risks)

II. Identification of Red Flags

A. Activities involving Identity Theft usually fall into one of the following five categories of red flags:

1. Alerts, notifications, or warnings from a consumer reporting agency
2. Suspicious documents (ID that looks forged or altered; the person presenting doesn't look like the photo or match the physical description; information on identification doesn't match what person is telling you)
3. Suspicious personal identifying information, such as a suspicious address
4. Unusual use of – or suspicious activity relating to – a covered account
5. Alerts from others (e.g., customer, identity theft victim, or law enforcement)(Please refer to Attachment A)

B. CHS facilities will be on the alert for the following possible red flag situations:

1. A complaint or question from a patient based on the patient's receipt of a:

   a) Bill for another individual
   b) Bill for a product or service the patient denies receiving
   c) Bill from a health care provider that the patient never patronized
   d) Notice of insurance benefits (or Explanation of Benefits) for health services never received.

2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.

3. A complaint or question from a patient about receiving a collection notice from a bill collector.

4. A patient or insurance company reports that coverage for legitimate healthcare services is denied because insurance benefits have been depleted or a lifetime cap has been reached.

5. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

6. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.

7. A notice or inquiry from an insurance fraud investigator for a private insurance company.

8. Any of the above should raise a red flag!

III. Detection of Red Flags

A. CHS has adopted the following procedures to aid in the detection of red flags for identity theft:

1. New Patient Accounts—This is when the potential for identity theft is most likely.
   a) Obtain appropriate identifying information and insurance information. This could be in the form of:
      i. Full name
      ii. Date of Birth

iii. Address
iv. Government issued ID/photo
v. Insurance card, etc.

- When possible, verify with the insurance company's information.

2. Existing Patient Accounts
   a) During each return patient registration, update the personal and insurance information listed above.
   b) Verify validity of requests for changes of billing addresses (utility company bill, etc.)
   c) Verify identification of customers before releasing any personal information.
3. Children—Observe for obvious discrepancies between the provided date of birth and the child's appearance. Verify the identity of the adult accompanying the child.(Please refer to Attachment B)

IV. Prevention and Mitigation of Identity Theft

A. In determining an appropriate response to a red flag or other threat of identity theft, CHS will consider risk factors that may heighten the possibility of identity theft, such as a data security incident that results in unauthorized access to a patient's account records or notice that a patient has become aware of someone fraudulently claiming to obtain medical services in the name of the patient.

B. Appropriate responses may include:
   1. Monitoring a covered account for evidence of identity theft;
   2. Contacting the patient;
   3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
   4. Reopening a covered account with a new account number;
   5. Not opening a new covered account;
   6. Closing an existing covered account;
   7. Not attempting to collect on a covered account or not selling a covered account to a debt collector;
   8. Isolating the encounter data/information until the identity is verified;
   9. Notifying law enforcement; or
   10. Determining that no response is warranted under the particular circumstances.
   11. Pre-registration / Central scheduling: Remind the patient that he/she will be required to show a photo ID and one other form of identification when presenting for service.

V. Updating the Identity Theft Prevention Program

A. CHS will evaluate the Program on an annual basis and will update the Program as necessary to reflect changes in risks to patients or to CHS from identity theft, based on factors such as:
   1. The experiences of CHS with identity theft;
   2. Changes in methods of identity theft;
   3. Changes in methods to detect, prevent, and mitigate identity theft;
   4. Changes in the types of accounts that CHS offers or maintains; and
   5. Changes in the business arrangements of CHS, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Administering the Program

A. The CHS Compliance Officer and the CHS Information Security Officer shall assume primary administration of the Program, subject to oversight by the CHS Board of Directors, including developing, implementing, administering, and periodically updating the Program.

B. The Compliance Officer/Information Security Officer shall be responsible for developing a facilities-wide training program for staff to educate them on the identification of, prevention of, and response to identity theft.

C. The Compliance Officer/Information Security Officer shall report to the Audit and Compliance Committee of the Board, at least annually, on our compliance with the Program. The report shall address material matters related to the Program and evaluate issues such as:

1. Any third-party service provider arrangements relevant to covered accounts;
2. Significant incidents involving identity theft and management's response;
3. Recommendations for material changes to the Program;
4. The effectiveness of the Program in identifying and addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts.

D. The Program shall be approved by the CHS Board of Directors.

VII. Investigating Red Flags Incidents

An Incident Report will be completed by the individual (or first contact). A team comprised of the compliance officer, information security officer, patient registration representative, patient accounting representative and security will be responsible for investigating any suspected identity theft incidents. Other individuals will be included depending on the location of the incident.

VIII. Training and Education

Identity theft can occur at any point of entry to CHS. It may also be discovered after the individual has been processed and through registration and receiving care or treatment as an inpatient or outpatient. Physician offices are also risk areas for identity theft. For these reasons, it is our intent to provide education to all employees at all sites within the Health System and CHI. Independent physician practices will be offered education as well, if they desire, because of the risk and negative impact to CHS from an identity thief who seeks care, treatment, and referral from an independent physician.

IX. Responsibility

The CHS Compliance Officer and Information Security Officer will be responsible for implementing this policy. The Directors/Managers of areas where covered accounts are opened or in existence are responsible for ensuring compliance with this policy.

4 Information Security – Program Requirements

SCOPE:

This policy applies to LifePoint Health and its affiliated Facilities and corporate entities (the "Company"). References to Facilities or Facility throughout this policy are meant to include all Company entities providing healthcare services.

PURPOSE:

To establish the general requirements for the Company and Facility Information Security Programs.

To establish the requirements for each Company-affiliated facility to adopt information security standards for the protection of electronic protected health information as required by the Health Insurance Portability and Accountability Act (HIPAA), Security Standards for the Protection of Electronic Protected Health Information (Security Standards), 45 CFR Parts 160, 162, and 164, all Federal regulations and interpretive guidelines promulgated there under, and all laws and regulations applicable to information security requirements.

This policy is the first in a series of Information Security policies designed to maintain the confidentiality, availability and integrity of Electronic Information Assets the Company owns or of which it is the custodian. The requirements of the HIPAA Security Standards form the basis of each policy in the series.

DEFINITIONS:

The following definitions apply to the Company Information Security Program and related policies and procedures.

Authentication - Verification of the credentials presented by Users (as defined below) to identify themselves to computer systems (i.e., corroboration that a person is the one claimed).

Data Classification - Please see Information Governance's Electronic Data Classification Standard.

Electronic Information Assets – For purposes of the Information Security Program, this includes, but is not limited to, the Company computer network; software applications, programs and data; hardware and equipment used to operate applications and programs or to create, store, process, or transmit data; and electronic medical devices that create, store, process, or transmit data.

Electronic Media - Electronic storage media including memory devices in computers (e.g., hard drives) and any transportable digital memory medium, such as a magnetic tape or disk, optical disk, or digital memory card; or transmission media (e.g., Internet, leased and dialup lines, and private networks) used to exchange information already in electronic format.

Information Security Incidents – Information security events that can include, but are not limited to:

- Attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with information system operations by individuals or computer programs;
- Network activity designed to result in unauthorized access, use, disclosure, modification, or destruction of information or interference with information system operations;
- Unauthorized use or disclosure of information or an information system by Users or computer programs;
- Disclosure or loss of a password, PIN (Personal Identification Number), token (e.g., card or device used for authentication), certificate (e.g., electronic digital certificate used to provide an electronic digital identity), or any mechanism that identifies the individual to computer systems or the facility (e.g., ID badge); and
- Damage to or loss of Company computer hardware (to include any portable or removable device such as Smart Phone, Tablet, Laptop, Cell Phone, USB Media, CD/DVD, etc.), software, or other electronic information

Information Security Guidance / Documents – Detailed requirements for a specific security topic. Guidance documents may:

1. Give additional information about an existing IS Standard, or requirement within a standard, in order to clarify that standard or requirement; or,
2. Provide foundational or interim information and requirements about a topic that is not yet a standard.

A guidance document does have a review process, but it is not as formal or lengthy as the formal governance process for a standard or a policy. The requirements in a guidance document may become part of a standard after those requirements complete the formal standards governance process. Facilities and Company workforce members must follow all requirements in a guidance document.

Information Security Policies – High-level requirements which support the mission and goals of the Information Security department. Policies travel through a governance process, which includes approval not only by Information Security but by Compliance and other key Company executives. Facilities and Company workforce members must follow all requirements in a policy.

Information Security Standards – Specific requirements which support a high-level policy. Approval of a standard goes through the official Information Security Standards governance process. Facilities and Company workforce members must follow all requirements in a standard.

Mobile Device - A communication device small enough to be carried in the hand or pocket and variously known as a smart phone or tablet. Mobile Devices considered in this Policy provide a broad range of services beyond simple telephony and are closer to mobile computers than legacy mobile phones. Examples of handheld devices: iPhone, iPad, Android, & Blackberry

LPNT Encryption Standard – This standard describes the company's strategy for encrypting sensitive data for transmission or storage and is for use in the United States and its territories only.

Principle of Least Privilege - The Principle of Least Privilege requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

User - A person who is authorized to use Company electronic information assets and electronic media, including but not limited to, employees, contractors, physicians, volunteers, vendor representatives, and business partners.

Workforce - HIPAA defines the workforce to include "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity."

POLICY

All Company-affiliated facilities must work to balance business needs and apply prudent measures to protect the confidentiality, availability, and integrity of Electronic Information Assets. In addition to implementing the Company information security policies in this series, each facility must implement and oversee the Company Information Security Program, as described within this policy, and develop and implement any information security procedures necessary to support compliance with applicable federal and state regulations. Facilities in states with additional requirements must develop and implement policies to comply with any state specific requirements that exceed the requirements of Company Information Security Policies. Information Security Policies and Standards are available within PolicyStat, accessible via the LifePoint Health SharePoint site.

Information Security Program Elements

The Company Information Security Program consists of policies, standards, procedures, and guidance provided by the LifePoint HSC (Health Support Center) Information Security Department within HITS (Health Informatics & Technology Services). The Facility Information Security Program includes implementation of the Company Information Security Program and any additional facility-specific information security procedures necessary to support compliance with applicable federal and state requirements.

The Company Information Security Program includes the following elements:

A. **Information Security Administration Procedures**

1. Procedures for granting access to electronic information assets, including access to physically secured areas housing the computer systems, must:

a. Validate User authorization;

b. Establish, maintain, and remove access in a timely manner; and

c. Follow the Principle of Least Privilege.

2. Requests for granting access to electronic information assets must be documented.

3. The Company and Facility Information Security Departments will establish information security administration policies, standards, processes, and procedures. Information security will be implemented and overseen by designated Facility Information Security Officers (FISOs).

a. The FISO is the key person for information security administration at the local facility and physician practice level, including oversight and implementation of the Company and Facility Information Security Programs.

b. Each Company-affiliated facility, pursuant to the Facility Information Security Officer Policy, LPNT.IS.SEC.006, must designate one individual to be the FISO. The FISO may delegate responsibility for department-specific information security procedures and application or platform-specific information security coordination to Local Security Coordinators (LSCs). c. Each Company-affiliated facility must also designate and train a sufficient number of LSCs to continuously meet Facility Information Security Program requirements. d. The FISO will use contemporary Information Security policies, standards, and toolkits as a basis for implementing the Facility Information Security Program. The Facility Information Security Program must comply with the Company Information Security Program.

B. **User Identification, Authentication and Use of Electronic Information Assets**

1. Users must be uniquely identified and authenticated when accessing electronic information assets. Credentials must be linked to an individual whose identity has been positively verified and validating information must be appropriately maintained.

2. Users must maintain the confidentiality of system credentials (e.g., user-IDs and passwords must not be posted, placed under keyboards, otherwise hidden, or shared).

3. Users are accountable and responsible for protecting electronic information assets residing on their assigned computer systems. Users must use reasonable precautions to physically protect equipment and Company electronic information (e.g., keeping computer screens from being visible to the public).

4. Users must comply with use and disclosure processes as if electronic information were paper and be accountable for executing appropriate agreements and/or obtaining required authorizations. 5. Accounts not associated with a specific User (e.g., service or machine accounts), must be protected by contemporary information security measures defined in the Information Security Standards.

C. Information Security Measures

1. Required information security controls must be installed, enabled, and maintained on each system, node, and/or communication component.

2. Established information security practices and methods must be followed when developing and installing system components. Measures must include, but are not limited to:

a. Uniquely identifying Users of a computer system or network node;

b. Authenticating Users to a computer system or network node in accordance with the Information Security Standards;

c. Providing mechanisms to support appropriate access;

d. Providing appropriate safeguards to monitor and log access to electronic information assets;

e. Establishing safeguards to ensure the confidentiality, integrity and availability of electronic information assets;

f. Providing authorized and secure communication connections for remote access and foreign network connection by approved Users;

g. Administering controls securely and in a timely manner;

h. Providing automatic log off procedures or processes;

i. Providing emergency access processes and procedures; and

j. Training of all Workforce members on information security measures.

3. Only the LifePoint HSC Information Security Department or an approved designee may acquire, possess, trade or use hardware or software tools that could be employed to compromise information security systems or probe for security vulnerabilities. Users must not test or attempt to compromise information system security measures. Bypassing or otherwise avoiding systems security measures, including compromise of such systems is prohibited.

D. Training

1. Each facility must have an ongoing training and awareness program to educate workforce members about the Facility Information Security Program. This training is also available through the LifePoint Health LifeTalent Center, accessible via the LifePoint Health SharePoint site.

2. The training and awareness program must include:

a. Information Security policies, standards, and guidance documents as its basis;

b. Initial and ongoing training for workforce members appropriate to carrying out their job-related duties;

c. Initial training within a reasonable period of time after an individual joins the workforce, preferably during orientation training; and

d. Documentation that training has been provided.

E. Risk Assessment

1. All critical information systems must be evaluated by the FISO and the LifePoint HSC Information Security department to determine the appropriate set of controls required to reduce risk to an acceptable level. System controls must be tested to confirm they operate as intended prior to implementation in a live environment.

2. Information Security risk assessments for electronic information assets must be performed on a periodic basis as determined by the Information Security Department. All major enhancements, upgrades, conversions, and related changes associated with any information system, application or software that will facilitate the use or disclosure of PHI, ePHI or Credit Card information must be preceded by a risk assessment as defined in the IT Risk Assessment & Management Standard.

F. Electronic Communications

1. Electronic mail, Internet, and network connection information security requirements are addressed in the Electronic Communications Policy, LPNT.IS.SEC.002.

2. Communication or transmission of electronic information outside of the LifePoint Health network must be in accordance with the Information Security Standards.

G. Physical & Environmental Controls

1. Electronic information systems (e.g., computer equipment, workstations and network devices) and network connections (e.g., access points) must be appropriately safeguarded from unauthorized physical access, tampering, or theft.

2. Access to locations in which electronic information systems are housed must be controlled and validated based on an individual's role or function.

3. Appropriate and effective environmental controls (e.g., fire protection and an uninterruptible power supply) must be implemented, utilized, and maintained to preserve and to protect electronic information systems.

4. Facility repairs and modifications to the physical components of a facility and locations related to physical security (e.g., hardware, walls, doors, and locks) must be documented.

H. Software Licensing

Software will be licensed in accordance with licensing agreements. Personal Computer (PC) Software Licenses are addressed in the PC Software License Management Policy, LPNT.IS.SEC.003.

I. Malicious Code Protection

1. Protection against viruses and other malicious code must exist at network points and on information systems where potentially infected messages or files enter, leave, or are stored. This includes, but is not limited to, a file or message:

> a. Passed to or from an outside network to or from the Company network, such as the Internet and vendor/business partner network connections;
>
> b. Residing for purposes of temporary data storage, such as e-mail mailboxes and file servers; and
>
> c. Accumulated as permanent data - stores such as file servers and workstations.

2. Appropriate malicious code protection must:

> a. Scan all messages and files in real time as data travels from/to foreign networks to the Company network (this is to be placed on the appropriate firewall or bastion host);
>
> b. Scan mailboxes, personal storage (PST) directories, and other permanent and temporary data storage locations on a regular basis;
>
> c. Provide a mechanism for centralized reporting of, and prompt response to, malicious code detected (e.g., a computer virus or worm); and
>
> d. Provide a mechanism to automatically update scanning software and pattern files used to recognize malicious computer programs on a regular basis.

3. Appropriate malicious code protection measures are specified in the Information Security Standards.

J. Mobile Computing

1. Requests to connect non-Company-owned devices to the Company network must be presented to the FISO or designee for review and approval prior to establishing network connectivity. All devices connected to the Company network must comply with the Information Security Standards. The connections must not expose the Company directly to external networks. Connectivity requests and the rationale for granting approval must be documented. The FISO or designee is accountable for the compliance of non-Company-owned device connections.

2. Mobile computing technology enables access to electronic information assets from within or out of the facility, with an increased risk of unauthorized disclosure. The FISO should raise awareness of the associated risks and enhanced information security measures must be applied. Users must implement appropriate safeguards to protect the information assets and act to prevent unauthorized disclosure of electronic information produced, retrieved, maintained, or disposed by mobile devices and/or working at off-facility locations.

3. Enhanced information security measures for working at off-facility premises (e.g., home offices, airports, hotels, and conferences) include but are not limited to:

> a. Company systems, access tools, and applications intended for Company business;
>
> b. Access and use of Company systems for work-related activities based on need-to-know;
>
> c. Each non-exempt, hourly employee is to access Company systems only during normal working hours unless approved in advance by his or her supervisor; and
>
> d. Termination or suspension of user access privileges and network connections to maintain the integrity and availability of the system.

4. Individuals using mobile devices containing Company information must take appropriate measures to protect these electronic information assets by methods such as:

> a. Using removable media (e.g., CD/DVDs, USB Media) and locking or securely storing the removable media when not in use;
>
> b. Not permanently storing Company information on an individual's non-Company PC;
>
> c. Follow the requirements for mobile devices as outlined in the LPNT.IS.SEC.011, Mobile Device Usage Policy;
>
> d. Deleting all Company information when the device is replaced or taken out of service; and
>
> e. Employing approved encryption software as outlined in the LPNT Media Controls Standard.

5. Users must return all Company equipment, information, supplies, or work products upon request or termination of privileges.

6. The Company's right to access files and messages, including on Non-Company owned equipment connected to Company systems, is addressed in the Electronic Communications Policy, LPNT.IS.SEC.002.

K. Disaster Recovery and Business Continuity IT Planning

Each facility must establish an appropriate Disaster Recovery plan for electronic information assets using a risk-based approach. The Disaster Recovery plan must establish procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, or natural disaster) that may damage electronic information assets. Access restrictions to backup information must be equivalent to that of the original electronic information. Disaster Recovery Planning (DRP) is addressed in the *Infrastructure Services Disaster Recovery IT Planning Standard.*

L. Information Security Incidents

1. Information security incidents must be handled and responded to in an appropriate manner. User access privileges and network connections may be suspended, if deemed necessary to maintain the confidentiality, integrity and availability of the computer systems. Please refer to LPNT IS.SEC.010 Protected Information Incident Response for information related to the appropriate investigation and remediation of potential information security incidents.

2. The HSC Information Security department manages the Company's reporting standards, and the processes and procedures for response to information security incidents. These standards, processes, and procedures address the following items:

a. Identification of information security incidents;

b. Reporting of information security incidents;

c. Responding to suspected or known information security incidents;

d. Mitigating harmful effects of known information security incidents;

e. Documentation of information security incidents and outcomes; and

f. Roles and responsibilities of the LifePoint HSC Information Security Department and its Incident Response Team(s), HSC Core Event Response Team, and FISOs.

3. Users, in collaboration with their FISO, must promptly report information security incidents upon discovery to the LifePoint Health Service Desk (1-855-744-4369).

4. The Information Security department incident response procedures may result in interruptions of network services, application access, or other resource availability if deemed necessary to maintain the confidentiality, integrity and availability of the computer systems.

M. Documentation

1. Each facility must develop appropriate system documentation describing safeguards that protect the confidentiality, integrity, and availability of electronic information assets. Documentation must include the following:

a. Disposal of electronic data; and

b. Access control procedures for granting different levels of access to electronic data based on the principle of least privilege.

2. Access to system documentation, including information security measures documentation, must be restricted based upon the sensitivity of the documentation and the individual's need to know.

3. Information Security Program documentation must be retained in accordance with the Company's Information Governance Policy.

N. Device and Media Controls

Facility processes and procedures governing the control of electronic media containing sensitive or restricted information must be implemented using HSC Information Security department developed Standards, including:

a. Final disposition of sensitive information and the hardware or electronic media on which it is stored.

b. Secure removal of sensitive or restricted information from electronic media before the media is made available for re-use.

c. Maintenance of records documenting movement of hardware and electronic media containing sensitive information and any person(s) responsible for such movement.

d. Backup of sensitive information before the movement of hardware or electronic media on which such information resides.

e. Employing approved encryption protocols as outlined in the LPNT Encryption Standard.

O. Sanctions

Suspected violations of this policy must be handled in accordance with this policy, the Code of Conduct, and any Company sanctions and enforcement policies. Investigation and resolution at the local level is encouraged and each facility must designate a process for promptly reporting violations. In addition, violations may be reported to the LifePoint Health Ethics and Compliance Line at 1-877-508-LIFE (5433).

P. Information Security - Security Committees

Each Facility must establish and maintain a Facility Security Committee (FSC), or equivalent committee (e.g., Facility Ethics and Compliance Committee) which is able to serve as an authority to which Facility security concerns and decisions are escalated and addressed.

1. The FSC, or equivalent committee, must be established and maintained in all Facilities in order to serve as a decision-making authority for Facility information security topics. The committee must be designated for oversight of all Information Security operations at each facility.

2. The FSC must meet at least quarterly and must establish procedures for recording and publishing minutes.

3. In order to adequately address concerns and effectively make decisions which impact the Facility, the FSC membership may include the following representatives:

a. FISO

b. HDIS (Hospital Director of Information Systems)/CIO (if different person than FISO)

c. Facility Administration Representation

d. Ethics and Compliance Officer

e. Facility Privacy Official

f. Health Information Management

g. Risk Management

h. Clinical Support

i. Physician Support

j. Nursing

k. Human Resources

l. LSC

m. Other (optional) (some suggestions: SCCM Administrator, Network Administrator, PC/Desktop Tech, Facility Management, Decision Support)

4. In addition to serving as a decision-making authority for Facility security concerns, FSCs must also:

a. Provide oversight to ensure the Facility is complying with LPNT Information Security Policies, Standards and Procedures;

b. Review required system appropriate access audits results, including actions taken for violations;

c. Review Hospital annual Information Security Risk Analysis and any remediation plans needed;

d. Monitor available security reports (e.g., Vulnerability Management Portals, Sarbanes-Oxley Act (SOX) Security Access Reports);

e. Establish procedures, guidelines, tools, and reports, for monitoring security functions;

f. Provide guidance for mitigating violations and recommend appropriate sanctions;

g. Provide guidelines and communication for implementing company, facility Information Security policies, procedures, standards, toolkits, and initiatives;

h. Develop, review and communicate local facility Information Security policies, procedures, standards, toolkits, and initiatives;

Q. Policy Exceptions

LifePoint HSC Information Security Department establishes information security governance processes. Exception approval is based upon risk management reflecting appropriate, reasonable, and effective information security measures for a given situation. Requests for exceptions from the requirements of this policy should be sent through LifePoint Health ServiceNow to the LifePoint HSC Information Security Department for formal review.

5. Information Security and Privacy Sanctions

STATEMENT OF POLICY:

Conemaugh Health System (CHS) complies with the Health Insurance Portability and Accountability Act. Because compliance is paramount, this policy establishes appropriate sanctions/discipline for workforce failure in complying with the organization's Information Security and Privacy policies and procedures.

REQUIREMENTS:

1. Conemaugh Health System's workforce members – including Employees, Employed Physicians, Residents, Temporary Employees, Students, Agency and Contracted Employees, Physicians, and Volunteers – are required to comply with its Information Security and Privacy policies and procedures, and violations will result in disciplinary action.
2. The level of sanction/discipline applied shall vary depending on the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of health information, and similar factors. The level of discipline is also contingent upon the work history of the individual. Categories of security and privacy violations are included in Appendix A of this policy.
3. Violations of a severe nature may result in notification to law enforcement officials as well as regulatory, accreditation, and/or licensure organizations; civil and/or criminal penalties may apply.

4. The policy and procedures contained herein do not apply specifically when workforce members exercise their rights as patients (including requesting access to their own medical information) in accordance with the HIPAA Privacy Rule, as detailed in the Conemaugh Health System HIPAA Privacy Plan.
5. The Compliance Office, in conjunction with Human Resources and the department manager, will investigate any allegations or wrongful actions and determine and apply the appropriate sanction(s)/discipline.
6. Workforce members will be sanctioned/disciplined in accordance with existing policies, contracts, or law enforcement:
   a) For employees, and temporary employees, failure to comply with CHS policies or procedures or with the requirements of the HIPAA Privacy and Security rules, sanctions will be applied as outlined in each entity's Corrective Action Policy.
   b) Physicians will be sanctioned/disciplined according to the Medical Staff By-Laws.
   c) Residents will be sanctioned/disciplined in accordance with appropriate Graduate Medical Education policies.
   d) Agency and contracted employees who violate CHS policies and procedures will be terminated from assignment at CHS.
   e) Students will be disciplined according to the performance rules of the appropriate school and may have their system access privileges temporarily or permanently revoked.
   f) Volunteers will be terminated from serving at CHS.
7. Certain violations may result in termination of employment or contractual arrangement without advance notice, including, but not limited to:
   a) Unauthorized release of confidential information.
   b) Theft of confidential data or computer equipment that could potentially compromise Conemaugh Health System's Protected Health Information.
   c) Willfully making erroneous entries in hospital computer records.
   d) Willfully introducing malicious code into the CHS network.
   e) Any grossly negligent, careless, or willful act which may result in personal injury, patient injury, or damage to hospital property or information.
   f) Accessing, downloading, or distributing information electronically that results in exposure of PHI, constitutes a copyright infringement, or is illegal.
   g) Tampering with Network equipment such as cabling networking equipment such as switches, routers, wireless routers, or other equipment CHS assets such as pc's printers, mobile devices such as phones etc.
8. All investigations and sanctioning/disciplinary actions will be documented and securely stored by the Compliance Office and will be retained for a period of at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.
9. The Compliance Office will notify law enforcement, regulatory, accreditation and/or licensure agencies of wrongful actions as appropriate.
10. If the sanctioning procedure results in suspension or termination of workforce members, the Compliance Office, in conjunction with the department manager, will ensure any necessary access changes are immediately made, including disabling computer accounts, and collecting electronic access cards and keys.

6. Information Security Program

POLICY STATEMENT

Conemaugh Health System (CHS) and its member organizations and affiliates (collectively "Conemaugh" or "CHS") are committed to conducting business in compliance with all applicable laws, regulations and CHS policies. CHS has adopted this policy to set forth its compliance with those standards established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regarding the security of Electronic Protected Health Information ("ePHI") (the "Security Regulations"). CHS's security program aims not only to comply with the Security Regulations, but also to incorporate generally accepted practices of information security in the healthcare industry.

The scope of this Policy covers CHS's general approach to compliance with the Security Regulations. As a covered entity under the Security Regulations, CHS must: (1) ensure the confidentiality, integrity and availability of all ePHI it creates, receives, maintains or transmits; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required; and (4) ensure compliance with the Security Regulations by its Workforce. Compliance with the Security Regulations requires CHS to implement:

- Administrative Safeguards – those actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of CHS's Workforce in relation to the protection of and authorized access to said ePHI.
- Physical Safeguards – those physical measures, policies, and procedures to protect CHS's electronic information system, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- Technical Safeguards – the technologies and the policies and procedures for its use that protect ePHI and control access to it.

REQUIREMENTS

The Information Security Program consists of personnel, processes and responsibilities as outlined in this policy and related policies, including:

A. **Acceptable Use of Technology Resources Policy**

The Acceptable Use of Technology Resources policy outlines authorized use of technology resources, including requirements for the following:

- Accountability and general responsibilities
- Physical requirements
- Internet and E-Mail use
- Password management
- Remote access
- Mobile/Portable devices
- Wireless access
- ePHI storage and transmission

- Other requirements

B. Information Security and Privacy Sanctions Policy

The Information Security and Privacy Sanctions Policy outlines actions which will be taken by CHS in response to various categories of security and privacy violations. The sanctions are based on the role of the individual within the CHS workforce, the severity, and intentionality of the violation.

C. HIPAA Plan Policy

The HIPAA Plan Policy outlines the CHS policy for complying with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) and Title XIII of the American Recovery and Reinvestment Act (ARRA) of 2009

Complaints

Corporate Compliance/Privacy Officer shall be responsible for facilitating a process for individuals to file a complaint regarding CHS's Privacy and Security Policies or the mishandling of ePHI and for ensuring that the complaint is appropriately documented and handled according to the CHS Security and Privacy Sanctions Policy.

Confidentiality and Security Agreements

The objective of requiring information confidentiality and security agreements is to provide awareness of the importance of information security and confidentiality and authorize and require agreements with individuals and external entities to protect CHS's information resources, including confidential patient information.

Information Confidentiality and Security Agreements with Individuals

1. All employees and other individuals granted access to information systems must sign and abide by the Confidentiality and Security Agreement ["Agreement"]. (See Appendix A.) The Agreement acknowledges specific responsibilities the individual has in relation to information security and the protection of sensitive information, including confidential patient information, from unauthorized disclosure.
2. Non-CHS physician practices, vendors, or other external entities may make and shall enforce such Agreements on behalf of employees working off-site (e.g., contracted transcription service, electronic claims submissions support contractor, physician office practice), if stipulated in the contract with the external entity (see Contracts with Business Partners below). Each individual working on CHS premises accessing CHS and/or patient information must sign an Agreement.

Contracts with Business Partners

Relationships with an external entity involving access to information systems or the exchange, transmission, or use of protected health information (PHI or ePHI) requires a fully executed Business Associates Agreement (BAA) as per the CHS HIPAA Plan policy.

1. The CHS standard BAA agreement form and associated HiTech Addendum form (if applicable) will be implemented whenever possible. These documents have been reviewed and determined to satisfy HIPAA requirements regarding business partner PHI safeguards.

2. Any business partner provided BAA version must be reviewed in advance by the CHS Privacy Officer prior to execution by the Privacy Officer. Business partner contracts require a BAA will not be executed until the BAA component has been satisfied.

Information Confidentiality and Security Procedures

1. The Confidentiality & Security Agreement form will be posted and maintained by MIS on the CHS Intranet under the Management Information Systems Department section.
2. Each employee must sign the Agreement at the time of employment and acknowledge the key tenants of the Agreement during the annual required education. The record of the complete agreement will be maintained in the individual's education and personnel records.
3. Physicians, allied health professionals, and physician office staff must sign the Agreement at the time information access is granted, and on defined intervals thereafter.
4. Each volunteer must sign the Agreement before beginning his or her service and at a defined interval thereafter. The agreement signature process and subsequent verifications can be completed during annual Required Education training (if the volunteer completes such training), volunteer orientation or separately. The completed agreement will be maintained with CHS's records of the volunteer's service.
5. Representatives of vendors and other external entities must sign the Agreement at the time information access is granted and at contract renewal, or, at defined intervals thereafter.

Documentation Requirements

All security related documentation must be retained for a minimum of six years by the appropriate security or compliance personnel (officer, coordinator, or administrator), Human Resources, or Corporate Compliance, including but not limited to the following:

- audit findings/reports
- signed confidentiality agreements (kept permanently)
- policies & procedures (for six years from the last effective date of the policy/procedure, including previous versions)
- security incident reports and supporting documentation
- process documentation such as audit program documentation
- risk assessment documentation
- risk mitigation documentation
- documentation related to decisions around whether or not to mitigate a risk
- sanctions documentation

Information Access Management

Workforce members and other users are granted access only to that health information to which they are authorized according to the procedures herein, in order to perform the particular function specified. Workforce members and other users shall use careful consideration to access and obtain only the type and amount of health information necessary to carry out the specified purpose. All Workforce members will be trained regarding appropriate access to ePHI, including the awareness of information access controls, and the minimum necessary requirement for accessing information.

Procedures for Access Authorization

1. Each supervisor or manager is responsible for ensuring that the access to requested PHI for each of his or her subordinates is the minimum necessary access required for each subordinate's role and responsibilities.

Information System Activity Review

CHS will implement internal audit procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. To ensure that system activity for all systems classified as medium, high, and severe risk is appropriately monitored and reviewed, each Entity must follow the minimum procedures outlined below:

1. Security incidents such as activity exceptions and unauthorized access attempts must be detected, logged, and reported immediately to the appropriate system management, security, and privacy officers in accordance with the Incident Response and Reporting section of this policy.

Incident Response and Reporting

This section covers the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes. A "security incident" is defined as "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system."

Handling of Retired Computer Devices and Storage Media

All computing devices and storage media MUST be returned to MIS when no longer actively used or upon replacement by new equipment. MIS will destroy the data and discard the obsolete equipment in accordance with the MIS Data/Device Destruction policy/procedure. The removal of any computing equipment/storage media (actively used or retired) from CHS property without approval is considered theft and will be processed as such. Under no conditions are retired computing devices to be disposed of in any way by any department other than MIS.

Reporting and Responding to HIPAA Security Incidents

All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of ePHI must be reported and responded to in accordance with the following procedures:

1. Users must notify MIS Help Desk immediately when a suspected computer virus/malware attack has been encountered or if computer theft or loss occurs or is suspected. User should also report any incident of possible unauthorized personnel access to MIS Data Communications rooms or observed tampering of computer equipment or computer/network equipment installation by unauthorized personnel. If an incident directly affects ePHI the user and/or MIS Help Desk must immediately notify the Privacy Officer.
2. Incidents may also be reported directly to the CHS Privacy Officer or Security Office, i.e., through the Employee Hotline.
3. Before involving outside authorities (i.e., police, FBI, media, etc.), Public Affairs, Risk Management and Legal Counsel must be contacted.
4. Corporate Compliance and Human Resources will investigate alleged security policy violations by workforce members and will apply sanctions in conjunction with the Department Manager, as outlined in the Information Security and Privacy Sanctions policy.

5. All correspondence with outside authorities such as local police, FBI, media, etc. must go through the designated person at each entity.

Documentation of Security Incidents

All HIPAA security related incidents and their outcomes must be logged and documented. The CHS Privacy Officer will also document and log incidents and outcomes related to HIPAA Security.

Periodic Evaluation of Security Policies and Procedures

The CHS Security Policies and Security Procedures shall be kept current in light of technological, environmental, or operational changes that could affect the security of ePHI or to ensure compliance with any changes in the law or applicable regulations. In the event that one or more of the following events occur, a policy/procedure evaluation will be immediately triggered:

- Changes in the HIPAA Security Regulations or Privacy Regulations
- New federal, state, or local laws or regulations affecting the privacy or security of PHI
- Changes in technology, environmental processes or business processes that may affect Information Security Policies or Security Procedures
- A serious security violation, breach, or other security incident occurs

Risk Management

All CHS networks, systems, and applications are subject to compliance with Information Security policies and procedures as defined in the Information Security Manual. Networks, systems, and applications that may send, receive, store, or access ePHI must also comply with the Information Security policies.

Roles and Responsibilities

1. CHS has designated an Information Security Officer with overall responsibility for the development and implementation of policies that conform to the Security Regulations ("Security Policies").
2. Corporate Compliance will oversee the implementation of the Security Program on an operational basis. The CHS Compliance Committee, the Audit and Compliance Committee of the CHS Board of Trustees, and the CHS Board of Trustees will each govern the program at the appropriate level of detail respective to their makeup. The Information Security Officer is responsible to communicate compliance status and implementation efforts to each of these groups. The Information Security Officer is also responsible to report security risks to these groups, especially those risks present due to an entity's lack of effort in complying with the established program.

Responsibility of All Employees within CHS

Every member of the CHS Workforce is responsible for being aware of, and complying with, the Security Regulations and the Security Policies and Security Procedures.

Sanctions, Mitigation and Non-Retaliation

CHS shall ensure that it mitigates damages for any violation of the Security Regulations and the CHS Security Policies and/or Procedures, applies appropriate discipline and sanctions employees and other Workforce members for any violation, and refrain from intimidating or retaliating against any person for exercising his or her rights under the Security Regulations or for reporting any concern, issue or practice that such person believes in good faith to be in violation of the Security Regulations or the CHS Security Policies and/or Procedures. CHS shall not require any person to inappropriately waive any rights of such person to file a complaint with the Department of Health and Human Services. CHS will sanction workforce members for policy violations according to existing disciplinary policies, as detailed in each entity's Information Security and Privacy Sanctions Policy.

Training and Awareness

1. The objective of the training and awareness program is to ensure that all workforce members are familiar with CHS's Information Security policies and their responsibilities regarding such policies.
2. Security training will be provided as follows:
    A. All new employees will receive Privacy/Security training as part of the new employee orientation. All employees receive new employee orientation within a reasonable time after beginning their employment.
    B. Annual Privacy/Security training will be included in each organization's required education program. All employees must receive the required education annually.

Workforce Security

The workforce is defined as follows: "employees (including temporary employees), volunteers, trainees, and other persons whose conduct, in the performance of work, is under the direct control of the entity, whether or not they are paid by the entity." Workforce members include but are not limited to: Employees, Employed Physicians, Residents, Temporary Employees, Students, Agency or other Contracted Employees, Physicians and Volunteers.

Termination Procedures

1. The Workforce member's supervisor or manager must ensure that all such Workforce member's accounts to access ePHI, including network and remote access accounts, are terminated.
2. The Workforce member's supervisor or manager must ensure that such Workforce member's access to all facilities housing ePHI is terminated, including but not limited to card access, keys, codes, and other facility access control mechanisms. Codes for key punch systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.
3. The Workforce member's supervisor or manager must ensure that all organizational assets capable of storing ePHI (e.g., notebook, portable devices, flash drives, PDAs) are retrieved prior to termination.
4. Human Resources and MIS must be promptly notified and the termination processed in accordance with the HR Termination Policy.
5. Access to ePHI is not extended to a Workforce member beyond the termination date of such Workforce Member's employment. Any exception to this requirement must be approved in writing by a senior leader and must define justification and a date/condition upon which access will be terminated.
6. Sudden terminations where system security is at higher risk should be called immediately to the Information Security Officer or any member of MIS leadership for immediate handling.

Access upon Transfer of Employment within CHS

If a Workforce member transfers to another department or workgroup within CHS:

1. The Workforce member's access to ePHI within his current Department must be terminated as of the date of transfer.

2. The Workforce member's new supervisor or manager is responsible for requesting access to ePHI commensurate with the Workforce member's new role and responsibilities.

RESPONSIBILITY

The Corporate Compliance and Management Information Systems departments are responsible for the implementation of this policy.

7. Privacy Breach Notification Policy

STATEMENT OF POLICY:

It is the policy of Conemaugh Health System (CHS) and its entities to comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996. To that end, the HIPAA Privacy policy was developed in 2003 and remains in effect. In 2009, the American Recovery and Reinvestment Act (ARRA) was signed into law. The ARRA included the Health Information Technology for Economic and Clinical Health (HITECH) Act as Title XIII of Division A and Title IV of Division B. The HITECH Act requires covered entities that fall under the HIPAA Privacy Rule, and their business associates, to provide notification in the case of breaches of unsecured protected health information (PHI). In January 2013, the Office for Civil Rights (OCR) released the HIPAA Final Omnibus Rule that revised some of the HIPAA and HITECH regulations and language. Privacy breach notification was one such revision.

DEFINITIONS:

Breach: The unauthorized acquisition, access, use, or disclosure of protected health information that compromises the privacy or security of that information. There are exceptions that may apply:

- Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the covered entity, if the disclosure was made in good faith.
- Inadvertent disclosure by one person at a covered entity or business associate who is authorized to access PHI to another person authorized to access PHI at the same covered entity or business associate, as long as the PHI is not further used or disclosed without authorization.
- It is a good faith belief that the recipient of the information would not have reasonably been able to retain the information.
- The impermissible use or disclosure of a limited data set as long as dates of birth or zip codes are not included in the data.

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained by a covered entity or its business associate in any form or medium.

Unsecured PHI: Any PHI that is not secured using a technology standard that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals. The technology standards published in the Federal Register in August 2009 include encryption and destruction as acceptable methods. The breach notification requirement only applies to breaches of unsecured PHI.

REQUIREMENTS:

Upon discovery **and** confirmation of a privacy breach, the extent of the breach will be determined through additional MIS audits and/or other investigatory efforts. This will include the number of individuals affected or potentially affected, the type of PHI involved, whether appropriate technical safeguards were in place, the likelihood of the information being adversely used, whether the breach was internal or external, and whether an exception to the breach notification rule applies.

If the breach was internal in origin, the department Manager and Director will be notified, and will meet with the employee to discuss the breach and obtain a written response from the employee regarding the reason for the inappropriate access. Human Resources will also be notified. If the breach occurred because of a theft, or is external in nature, the Security Department and law enforcement will be notified, if indicated. Marketing and Communications, Human Resources, Senior Leaders, Medical Records, and legal counsel will be notified as needed.

In keeping with the Final Rule, any impermissible use or disclosure is presumed to be a breach. The covered entity must notify the individual (s) affected unless an exception applies, or the covered entity demonstrates through a risk assessment that there is a low probability that the PHI has been or will be compromised. The four factors that must be assessed include the following:

1. The nature and extent of PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

If we cannot demonstrate a low probability that the PHI has been compromised, then the affected patients must be notified. The risk assessment will be documented and retained in the investigation folder.

A notification letter will be sent by first-class mail to the affected individuals within 60 days of the discovery of the breach. The notification letter will include the following information:

- Brief description of what happened, including the date of the breach and the date of discovery of the breach, if known
- Description of the types of PHI that were involved in the breach, for example whether full name, social security number, date of birth, home address, diagnostic tests, treatment, disability code and other information were involved
- Any steps the individuals should take to protect themselves from potential harm resulting from the breach, including an offer of credit monitoring for a specified time period, at no charge to the individual
- Brief description of what the covered entity (CE) is doing to investigate the breach, mitigate risk to the PHI, and protect against any future breaches
- Contact procedures for the individuals to ask questions or obtain additional information, which should include a phone number, email address, web site, or postal address

Breach notification letters will be sent to the affected individual except in the following situations: If the affected individual is deceased, the letter will be sent to the known next-of-kin or personal representative/agent; if the affected individual is a minor, the letter will be sent to the parent or guardian.

SPECIAL CONSIDERATIONS:

If the breach involves 500 or more individuals, in addition to the affected individuals being notified, press releases regarding the breach will be sent to prominent media outlets covering the regions that CHS serves. Additionally, notice will be posted to the CHS website and the Department of Health and Human Services (DHHS) will be notified immediately.

If fewer than 500 individuals are affected by the breach of unsecured PHI, it will be included in the annual log to DHHS, which is submitted within 60 days after the end of the preceding calendar year.

In the process of sending the notification letters, if there is insufficient or out-of-date contact information for 10 or greater individuals, a substitute notice will be posted to the CHS website and include a toll-free phone number that individuals may call for further information.

A substitute notice may also be provided if the cost of breach notification exceeds $250,000 or if the affected number of individuals exceeds 500,000. Substitute notice consists of all of the following: email notice if available, conspicuous posting on the CHS website, and notification to major media.

RESOLUTION / RECOMMENDATIONS:

Once the employee provides a written response regarding the records breach, the internal team -- Compliance/Privacy Officer, MIS Security Officer, HR Employee Relations representative -- will review the response and make a recommendation to the Manager, Director, and/or appropriate Senior Leader, if warranted.

RESPONSIBILITY:

The Corporate Compliance/Privacy Officer, in conjunction with the MIS Security Supervisor and the Employee Relations representative, are responsible for the enforcement of this policy.

8. Credit Card Handling Policy and Procedures

STATEMENT OF POLICY:

It is the policy of the Conemaugh Health System (CHS) to adhere to all credit card processing security rules outlined below and developed by the Payment Card Industry (PCI) Data Security Standards. Due to the increased threat of identity theft, fraudulent credit card activity and other instances where cardholder information has been compromised, the credit card associations (Visa, MasterCard, Discover, etc.) have mandated compliance to these standards for any merchant or service provider that "transmits, stores, or processes" cardholder information. CHS is dedicated to maintaining PCI Compliance in order to maintain the ability to accept credit cards for payment and to safeguard credit cardholder information provided by our patients and customers.

I. SCOPE - This policy applies to all subsidiaries of CHS. For Joint Ventures, the standard will be applied to the greatest possible extent based on direction from management of the joint venture.

II. STANDARDS - Credit card processing (e.g., on-line, by phone, card swiping) should conform to requirements of the law and follow specific security rules outlined below and developed by the PCI Data Security Standards. Failure to follow the requirements below can result in severe penalties, including fines and prohibition from further acceptance of credit cards:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software and programs
- Develop and maintain secure systems and applications

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

While the CHS MIS Department is responsible for addressing the majority of the above listed requirements, it is important that personnel who are authorized to accept credit card payments be aware of the requirements and receive guidance relative to the items that specifically apply to their operational procedures such as restricted access and data collection and retention.

III.PROCEDURES - Credit card information such as cardholder name, signature, account number, card type and expiration date should be kept secure and confidential:

- Do not store on any computer, electronic device, or network
- Do not transmit in an unsecure manner such as unsecure fax or email, or interoffice envelope
- Access must be limited to appropriate and authorized personnel responsible for posting payments
- All personnel handling credit card information will complete CHS's annual required education for Health Information Privacy and Security and will agree, through the signing of the Health System Confidentiality Notice, not to inappropriately disclose or acquire any information regarding the cardholder's account.
- All documentation containing credit card information must be destroyed in a manner compliant with CHS's HIPAA policies.
- In instances where credit card information needs to be retained, retention must not exceed the useful life of the payment, or no longer than 3 months
- Short term retention of documentation should be housed in a secure area such as a locked drawer, locked file cabinet or locked safe
- Once the retention period ends, the information should be shredded according to the Health System Record Retention Policy.
- Personnel may use the attached approved Credit Card Payment Form when obtaining credit card information via telephone for processing and unless retention is needed, the form shall be shredded immediately following processing.

IV. OTHER - A periodic review of Credit Card Handling procedure and adherence to PCI Data Security Standards will be conducted by CHS's Internal Audit Department. All Subsidiaries must be compliant with all policies and procedures as outlined herein.

9. User Account Management Policy

The purpose of this policy is to help ensure user accountability and minimize the risk of unauthorized access to computer resources. Only active user accounts are to reside on the computer systems. This standard applies to any information system or application which controls access to confidential or restricted data.

A user ID is a unique identifier that allows a person to access Company information systems. Each user ID is for use by a single person. A person's user ID provides access to all systems for which he/she has access approvals from the owner. Each user is to be uniquely identified and authenticated (e.g., no Generic User IDs) when accessing sensitive electronic information assets. However, due to business requirements, generic user IDs may be necessary for granting access to shared workstations (e.g., Point of User application). Users are to maintain the confidentiality of access methods (e.g., user IDs and passwords will not be posted, placed under keyboards, or shared at any time).

Most operating system and security software have user IDs predefined by the software developer, which allows the user ID to perform wide-ranging functions, including installing, changing, and deleting software functions as well as granting other users access to information and system functions. All software/system-supplied accounts (such as a guest account) should be removed. If these accounts cannot be removed, minimize security exposure by renaming the account, changing the password, and/or deactivating the account. If someone must know the password, the appropriate system owner/administrator must be contacted to establish the appropriate process and procedure.

SCOPE

This policy applies to all accounts (or any form of access that supports or requires User/Network ID) on any system that resides at any company facility, has access to the company network, or stores any non-public company information.

PURPOSE

To define a standard process for managing various types of accounts and passwords for these accounts that have access to Conemaugh Health System information systems and technologies.

GENERAL

The Information Systems Security Team (ISST) is responsible for ensuring that this policy is adhered to. All authorized users will be provided a unique User/Network account for their sole use. All accounts must be uniquely identifiable by an assigned username. All accounts must have a password that complies with the Password Policy. Accounts will be administered by a Security Administrator. Accounts will be managed based on their assigned category as follows and as defined on Attachment A – Account Management Settings Table.

Creating and Granting Access to User Accounts

A user account may only be provided to a user under the following conditions:

a. New Hires upon receipt of Boarding Pass email notification from Human Resources (HR) will be granted email accounts only. The following Standards will be adhered to for additional application access as defined by job title.
b. Standard Application Accounts for Nursing Personnel New Hire Clinical
c. Standard Application Accounts for Physicians and Allied Health Professionals
d. The user's one up manager or the responsible business owner Director will need to submit an authorized Security Access Form [SAF] to ISST to apply for system access.
e. A user account is assigned to a valid individual. The person or entity must have a valid business relationship such as an employee, contractor, or business partner.
f. The user has signed a Confidentiality and Security Agreement (CSA) acknowledging his/her role and responsibility in the protection of electronic information assets.

Procedures for granting access must be based upon the principle of least privilege, providing users with the minimum amount of information needed to complete a task or job responsibility.

The ISST will create the user ID and assign a temporary password. Users are required to change password upon login and adhere to complex password policy requirements.

10. Electronic Data Storage and Backup Standard

SCOPE

This policy applies to all subsidiaries and affiliates of LifePoint Health, Inc (the “Company”) and all employees of any of them.

PURPOSE

The purpose of this policy is to safeguard data in the event of hardware or software failure, virus or other data corruption threat, or destruction by physical threats (such as by fire or flood), and to enable recovery of data upon loss locally.

LifePoint recognizes that the backup and maintenance of data for applications and servers are critical to the viability and operations of our hospitals, physician practices, and our departments across the HSC. It is essential that LifePoint adhere to the following policy to ensure that data files are backed up on a regular basis.

This standard is applicable to all facilities affiliated with LifePoint Health (the "Company"), including, but not limited to, hospitals, ambulatory surgery centers, home health agencies, physician practices ("Facilities"), as well as all corporate departments.

DEFINITIONS

Replication: replication is the process of copying data over a storage area network (SAN), local area network (LAN), or wide area network (WAN). Replication ensures consistency between two data stores by copying the data bit by bit between the two and is often used for disaster recovery purposes where an active copy of the data would be needed in an expedited time period should a failure ever occur on the primary data store. Synchronous replication ensures transactional currency of the replicated data, while asynchronous data is refreshed on a scheduled basis.

Confidential and Restricted Information: Confidential and Restricted Information includes data that, if disclosed, could result in damage to the company, an individual, or other stakeholders. It can include passwords, social security numbers, protected health information (PHI), financial data such as bad debt records, and our employees' human resources files. See the Electronic Data Classification Standard for more information.

Media: Any electronic asset, regardless of ownership, that has the potential to store, process, or transmit Company information.

Portable Device: Electronic media that is designed for mobility, such as laptop computers, tablet computers, cameras, smart phones, or personal digital assistants (PDAs).

Removable Media: Electronic media that can be easily removed from a system, such as USB ("thumb") drives, memory cards, CDs or DVDs, video tapes, backup tapes, "hot swap" server drives, or external hard drives.

Cloud Computing: a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.

STANDARD

Backup Data Management

1. Backups must be verified/tested to ensure that the backup versions are readable and can be restored within the critical timescale for all critical applications.
2. Backup files or media shall be stored in a secure manner in a controlled-access location at least 5 miles from the location of the primary data. The storage location must be accessible seven (7) days a week/ twenty-four (24) hours a day.
3. The backup storage site must be physically secured and environmentally protected (e.g., air conditioning, humidity controls, fire resistance). Access to backups must be restricted to authorized personnel. Please refer to the Physical Access Controls Standard and Environmental Controls Standard.
4. If physical backup media is used, it shall be stored offsite a location in accordance with the Environmental Controls Standard.
5. Critical magnetic media should be stored in a vault, safe or equivalent that is fire resistant at all times.
6. Only an approved HPG record management vendor, HSC, a separate LifePoint managed hospital or practice, or an approved cloud storage vendor are permissible for secure storage of backups
7. Backups must be transported to the off-site area in a secure manner. Please refer to Media Controls Standard.
8. For all production systems, at least one complete backup equivalent (all modules) per month shall be kept securely off-site.
9. Other backups, such as incremental backup copies, may be housed on-site in a secure location with controlled access.
10. All backup media shall be treated with the same care and security as the live data from which it was derived.
11. Destruction and re-use of backup media shall follow the Media Sanitization Standard, Disposition of Information Standard and Procedures and Media Controls Standard. (These standards can be found online on PolicyStat).
12. Backups must be time-stamped, reconciled to live versions, and retained for at least three backup generations. Backups must be clearly and accurately labeled and protected from accidental overwriting. A copy of the documentation (e.g., date, contents of tape, etc.) Pertaining to the backup should be stored with each backup.
13. Transmittal records of the movement of storage media (magnetic tape, removable optical or magnetic disks, cartridges, or solid-state drives) to or from an off-site storage center must be maintained at two separate locations.
14. In the event that storage media must be discarded, please refer to the Media Controls Standard.
15. Data replication (synchronous or asynchronous) that occurs to an offsite location does not meet the definition of a backup (see Definition).
    a. Cloud backup storage solutions may be utilized providing that they meet the following criteria:
    b. Cloud Vendor has been approved by LifePoint HSC Technology Review Board.
    c. Cloud Vendor has been approved by LifePoint Third Party Data Release Process.
    d. Cloud Vendor has executed a BAA for any EPHI data that may be stored in the cloud.

Backup Retention

1. Backups must be verified/tested to ensure that the backup versions are readable and can be restored within the critical timescale for all critical applications.

2. Backup files or media shall be stored in a secure manner in a controlled-access location at least 5 miles from the location of the primary data. The storage location must be accessible seven (7) days a week/ twenty-four (24) hours a day.
    - Weekly Full System Backup Copies – Retained for 30 days
    - Monthly Full System Saves – Retained for 60 days
    - Quarterly Full System Saves – 2 years
    - Annual Full System Saves – 7 years

End-User Devices

1. In the event that storage media must be discarded, please refer to the Media Controls Standard.
2. Data replication (synchronous or asynchronous) that occurs to an offsite location does not meet the definition of a backup (see Definition).

Network Shared Drive Storage

1. Network drive space is a company resource provided for the purpose of storing work-related documents and files.
2. Users have a responsibility for managing this space, which includes deleting non-essential or obsolete files in order to keep space utilization at a minimum.
3. Workstation (local) drives (the C: drive or similar), as well as temporary external storage devices/removable media (such as CD/DVDs, USB drives, etc.) are not acceptable for storage of company data and are not recoverable. In the event of equipment failure, there is the potential for loss of data.
4. Work-related critical information shall be stored on designated network file server locations.

Applications Data and Storage

1. The business owner of the application must define system backup requirements based on the information classification or the function of the information system resource.
2. Back-ups must be made of master files/databases, transaction files, system program/utilities, application software, parameter settings and system documentation.
3. Back-ups must be made frequently enough to meet the time-criticality of business processes
4. At a minimum, full backups must be executed weekly.
5. Backups must be made on separate physical tapes or disks.

11. Encryption Standard

Standard

Data encryption is used to control access to information, protect the integrity of transactions, disguise data during transmission, and authenticate the users and devices of an information processing system. Encryption techniques are used to protect against the risks associated with the transmission and storage of confidential or sensitive information. Reversing the process of encryption, which transforms the cipher back into readable data, is called decryption. Keys are an essential part of authentication and data encryption processes. Authentication and encryption keys are short sequences of numbers or characters that are selected or electronically generated by hardware devices. Since most encryption algorithms are published and well known, the security of the data being processed is dependent upon the secrecy of the key. The destruction or loss of the key is equivalent to the loss or destruction of the data itself. This standard outlines LifePoint Health requirements when using encryption to protect sensitive data during transmission or storage.

This standard does not address wireless local area network (WLAN) requirements. For more information about WLAN requirements, please see the Wireless LAN WPA Standard.

For information about specific requirements for storing or transmitting sensitive data, see the following standards*: Electronic Transmission Standard, Media Controls Standard, Internet Security Standard, and Third-Party External Connectivity Standard.*

Encryption requirements are as follows:

1. Asymmetric encryption:
   - should use 3072-bit keys, if possible
   - must use at least 2048-bit keys
2. Symmetric encryption:
   - must use 128-bit keys
   - acceptable to use 168-bit keys for 3DES
3. Elliptical curve encryption:
   - Must use 224-bit keys
4. Hashing must be, at a minimum, 160-bit (e.g., SHA-1, SHA-256)
5. Encryption keys must have a stated life and should be changed on or before the stated expiration date.
6. The secrecy of any encryption key must be maintained until all of the information being protected is no longer considered confidential.
7. LifePoint Health encryption systems must be designed so that no single person has full knowledge of any single encryption key. This must be achieved by separation of duties and dual control.

Note: encryption key lengths will be re-evaluated on an annual basis and adjusted, as necessary. Acceptable key lengths will be based on *NIST Special Publication 800-78 Cryptographic Algorithms and Key Sizes for Personal Identity Verification.*

Procedures (Tools and Techniques)

See SharePoint for related procedures and resources.

Monitoring

The Hospital Director of Information Systems (HDIS) and Facility Information Security Officer (FISO) will monitor the Encryption Standard for compliance and update related facility processes, as necessary.

Responsibility

It is the responsibility of the HDIS and FISO to ensure implementation of the Encryption Standard.

12. Electronic Transmission Standard

Scope

These requirements apply to all workforce members who access Sensitive or Restricted Data.

Purpose

These requirements help protect LifePoint Health data which is transmitted through messaging systems, such as MOX, Outlook; as well as other types of transmissions. These requirements support federal regulations, state laws, and contractual obligations.

Standard

1. Workforce members must protect Sensitive Data which they send through electronic transmissions.
2. Workforce members must encrypt emails or other transmissions containing Sensitive Data when sent to a recipient who is external to the LifePoint Health network, by including [encrypt] in the Subject line.
    a. Appointment reminders sent to consenting patients do not need to be encrypted, provided that the reminders only include facility name, telephone number, date, and time. See Company HIPAA & Privacy policies for guidance on Patient Privacy & Confidentiality.
3. Workforce members must not include Sensitive Data in the subject line of an email.
4. Workforce members must not send Sensitive Data in text messages (SMS protocol) or to text pagers through applications not approved by LifePoint Health.
5. Workforce members must not use electronic messaging systems to send Restricted Data.

13. Media Controls Standard

Purpose

Electronic media is capable of holding large amounts of Company data. As such, all electronic media merits formal security standards and procedures in order to appropriately protect the Company's information and assets. Such standards and procedures will also help protect the Company from malware that so easily spreads through all forms of media, posing a significant external threat to Company systems.

This standard covers access control, accountability, release, storage, backup, disposal, and off-site maintenance relating to the facility's electronic media, in support of HIPAA Security Rule compliance.

Terminology

For the purpose of this standard, the following definitions apply.

Media: Any electronic asset, regardless of ownership, that has the potential to store, process, or transmit Company information, excluding servers and server drives. (For information about server security requirements, including "hot swap" server drives, please see the Server Security Standard.)

Portable Media: Electronic media that is designed for mobility, such as laptop computers, tablet computers, cameras, smart phones, or personal digital assistants (PDAs).

Removable Media: Electronic storage media that can be easily removed from a system, such as USB ("thumb") drives, memory cards, CDs or DVDs, video tapes, backup tapes, or external hard drives.

Company-owned Media: For the purpose of this standard, Company-owned media includes all electronic media owned or leased by the Company.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a facility, is under the direct control of such facility, whether or not they are paid by the facility.

Sensitive and Restricted Information: Sensitive and restricted information includes data that, if disclosed, could result in damage to the Company, an individual, or other stakeholders. It can include passwords, social security numbers, protected health information (PHI), financial data such as bad debt records, and our employees' human resources files. See the Electronic Data Classification Standard for a more detailed description.

Standard

Media Management and Information Handling

1. Workforce members must only use Company-owned media to store, input, transmit, and transfer Company data.
2. Workforce members must never connect Company-owned media to non-Company-owned media (e.g., a Company-owned USB drive must not be connected to a personally owned computer, and a personally owned USB drive must not be connected to a Company-owned computer).
3. The procedures for access to and distribution of removable and portable media must include the following:
    a. Inventory of Company-owned removable and portable media authorized and assigned to workforce members (whenever possible) or departments (in those cases where a workforce member cannot be identified);
    b. Records of external recipients of Company-owned removable media containing sensitive or restricted information;
    c. Review of the above workforce members and recipients on a minimum of an annual basis to validate access to such media is still warranted, with results reported to the facility's Compliance Committee; and
    d. Documented initial and annual education of the above workforce members regarding all applicable portable and removable media controls.

Additional Controls for Removable Media

The following controls only apply to removable media.

1. Sensitive or restricted information stored on or transferred to removable media must be encrypted using whole disk or file-level encryption whenever possible.
2. If Sensitive or restricted data cannot be encrypted for a business reason (e.g., submission to a government entity that does not support encrypted submissions), or technical limitations hinder a workforce member's ability to encrypt the data, approval must be obtained by Corporate IT and the exception must be documented by the facility, accompanied by the physical security measures implemented to protect the media.
3. In the event that an exception is approved and unencrypted removable media containing sensitive or restricted data must be sent off-site, physical transport of the media must:
    a. Be through reliable couriers (e.g., bonded); facility management must determine a list of approved couriers;
    b. Have the ability to confirm the receipt of media to the intended party and track location of media; and
    c. Be enclosed in a locked container whenever possible. If a locked container cannot be used, tamper-evident packaging must be used and the reason for not using a locked container must be documented by the facility and approved by Corporate IT.

Additional Controls for All Other Media

The following controls apply to all media except removable media.

1. Media containing Sensitive or restricted information must be whole disk encrypted whenever possible.
2. If media containing Sensitive or restricted information cannot be whole disk encrypted:
    a. The media must be protected by passwords;
    b. Workforce members using such media must encrypt individual files containing Sensitive or restricted information whenever possible;
    c. If technical limitations require unencrypted sensitive or restricted information to be stored, processed, or transmitted on unencrypted media, the facility must obtain approval from Corporate IT and document the exception and the physical security measures implemented to protect the media.

Storage, Backup and Destruction of Electronic Media

1. Media must be stored in a secure and environmentally protected area in accordance with the Physical Access Controls Standard and Environmental Controls Standard.
2. Media must be backed up in accordance with the Disaster Recovery IT Planning Standard.
3. Media must be disposed of in accordance with the Media Sanitization Standard (full standard on PolicyStat).

Off-site Maintenance

If media containing sensitive or restricted information must be released for off-site maintenance, a legally binding contract must be in place between the Company and the vendor. Contract language must state that the vendor must follow the data handling, storage, and disposal requirements pursuant to Company and facility policies and standards.

Reporting a Loss or Theft

Workforce members must immediately report all suspected losses or thefts of media containing Company information in accordance with LL.025 Response Protocol for Potential Data Security Events Policy and HIPAA.GEN.007 Protected Health Information Incident Response Policy.

Monitoring

The Facility Information Security Official (FISO) must monitor the Media Controls Standard for compliance and changes and update related facility processes, as necessary.

Responsibility

It is the responsibility of the FISO to implement the Media Controls Standard.

It is the responsibility of executive management to enforce compliance with the Media Controls Standard.

13. Media Sanitization Standard

(Full policy can be found on Conemaugh PolicyStat website)

Terminology

Media Sanitization: The process of removing data from electronic media so that it cannot be recovered. Data sanitization includes both clearing and destroying media.

Wiping: A media sanitization process that removes data while leaving the media intact and reusable. Also known as overwriting or clearing, this method uses a software program which overwrites all of the data on the drive with random bits. Media that has been cleared in this way can only be recovered through expensive laboratory attacks.

Destroying: A media sanitization process which involves the physical destruction of the media. Destruction can be accomplished via one of several means, such as incineration, melting, pulverizing, or shredding. Data that is destroyed through these physical destruction methods cannot be recovered in a laboratory attack.

Degaussing: A media sanitization method which uses a magnetic field to erase the data held on magnetic media, such as hard drives, diskettes, and tapes. Data that has been degaussed cannot be recovered in a laboratory attack. Hard drives that have been degaussed cannot be reused, unlike some media types, such as diskettes. Optical media types, such as CDs and DVDs, cannot be degaussed.

Standard

This standard outlines requirements for removing electronic data from hard drives and removable electronic media prior to disposing of, transferring, or reusing the electronic media. This includes any Company system or device which contains a hard drive, such as Company servers, desktops, laptops, clinical systems, printers, or copiers. This also includes electronic removable media such as CDs, CD-RWs, CD-Rs, USB (“thumb”) drives, memory sticks, ZIP disks, floppy disks, and backup media.

Note: For the majority of electronic media types, simply deleting a file or folder does not remove the data from the media and does not fulfill the requirements of this Standard. There is a limited exception defined in the “Requirements for Electronic Media Reallocation” section of this Standard in the case of re-writable CDs and DVDs.

1. Facilities must sanitize all electronic media before it leaves facility ownership or is transferred, transported, repurposed, or reallocated in any way.
2. Facilities must develop and implement processes to physically protect electronic media prior to sanitization.
3. Facilities must sanitize media using one of the approved methods outlined in this standard.
4. Facilities must physically destroy or degauss all media that is not fully functional prior to disposal.
5. If your facility contracts with a third party to sanitize media, you must have a formal contract in place. A Certificate of Destruction must be provided by the third party as applicable.
6. When sanitizing electronic media containing original business records, you must complete a Certificate of Destruction per the Records Retention Policy, EC.010. Note: This only applies to the destruction of original electronic business records, not electronic copies of records. See EC.010 for more information regarding the Company’s record retention requirements.
7. In order to ensure that electronic media is properly sanitized, each facility must appoint one individual as the person responsible for the disposal and reallocation of electronic media, referred to as the Media Sanitization Point of Contact.

14. Disaster Recovery IT Planning Standard

Note: When complying with this standard, facilities should perform an application assessment identifying critical business applications. After creating the prioritized listing, facilities should consider applications residing on facility servers versus applications residing on LifePoint HITS or Service Provider servers. The facility should perform a gap analysis between local facility disaster recovery plans and LifePoint HITS or Service Provider plans to ensure critical applications are included in the appropriate recovery plan and to help reduce redundancy in recovery procedures (i.e., identify facility recovery responsibilities and LifePoint HITS or Service Provider recovery responsibilities).

Standard

In the event of a disaster, natural or man-made, failure to have an executable IT Disaster Recovery Plan (DRP or Plan) will delay recovery of operations. The DRP must be clearly written and outline comprehensive operational details. Each facility must have a clear understanding of its tolerance for downtime and verifiable resources for its DRP, to avoid potential delayed or unsuccessful recovery. This guideline addresses the development and maintenance of a comprehensive IT Disaster Recovery Plan.

Requirements from the HIPAA Security Rule

The rule requires that each covered entity have a contingency plan for responding to events that disrupt systems containing electronic health information. Plans must include:

1. A data backup plan for creating and storing copies of electronic health information (required).
2. A disaster recovery plan for restoring lost data (required).
3. An emergency mode operations plan for continuing critical business processes during emergencies (required).
4. Testing and revising of contingency plans (addressable).
5. An applications and criticality assessment (addressable).

Business Impact Analysis (BIA)

1. Assess the criticality and sensitivity of computerized operations and identify supporting resources. These resources may include computer resources, such as computer hardware, software, and data files; computer supplies, including paper stock and pre-printed forms; telecommunications services; and any other resources necessary to the operation, such as people, office facilities, and supplies.
2. Identify the key business processes to be protected by the DRP.
3. A set of scenarios for possible disasters and the assessments of the business impact of such scenarios must be documented within the DRP. The identification of scenarios will help a facility develop a Plan to address the wide range of things that can go wrong.
4. Business owners must prioritize business applications, including the servers' physical location (e.g., hosted service provider, HITS data center, facility, etc.), and identify thresholds for acceptable downtime. Factored into this should be the identification of the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the facility of the continued unavailability of the resource.
5. The recovery timescales for critical applications and computerized operations must be signed off by the business owners (senior management).

Backup Requirements

1. The business owner must define system backup requirements based on the information classification or the function of the information system resource.

2. Back-ups must be made of master files / databases, transaction files, system program / utilities, application software, parameter settings, system documentation and any other data or artifacts required to fully restore the system to operation.
3. Back-ups must be made frequently to meet the time-criticality of business processes, especially with regard to the Recovery Point Objective (RPO: the point in time to which the system will be restored).
4. At a minimum, incremental backups must be executed on critical information system resources daily and full backups must be executed monthly. However, the backup schedule should provide for full backups frequently enough to ensure the ability to meet the Recovery Time Objective (RTO: the full elapsed time it will take to restore the system to operations).
5. The business owner or system administrator must develop an off-site backup rotation and retention schedule of all locally supported systems that meets these requirements
6. The management of backups throughout their lifecycle, including storage, retention, and destruction, must adhere to the LifePoint Electronic Data Storage and Backup Policy.
7. Guidance on the development of RPOs and RTOs is addressed in the Business Continuity IT Planning Standard.

Data Replication

1. Restoration of systems from backups often does not support the desired Recovery Time Objectives (RTOs) for critical systems. In these cases, replication of data to the alternate recovery site may be required.
2. Replication is a form of high availability that can significantly improve RTOs, however in most cases it is not a substitute for traditional data backups. Backups should be managed in accordance with the Electronic Data Storage and Backup Standard.

Critical Document Components

Senior Management commitment and Plan approval

1. Senior management must approve the documented DRP in writing.
2. Key affected groups, including data center management, and program managers must also approve the documented DRP in writing.

Plan distribution

The DRP must be distributed to all appropriate personnel including all individuals who would require the Plan in case of an emergency, such as the Disaster Recovery Team members.

Roles and responsibilities

1. The Plan must clearly assign responsibility for recovery and indicate where coordination is required between hospital IT and HITS staff, as well as key vendor partners.
2. The Plan must allow implementation independent of specific individuals.
3. Disaster Recovery Team members and their alternates must be informed of and trained in their responsibilities and equipped to fulfill them, including appropriate security authorization.
4. The description of responsibilities, technical design and recovery procedures must be specified in sufficient detail to be followed by individuals who do not normally carry them out.
5. The core group of people responsible for the execution of the DRP, the Disaster Recovery Team, should be comprised of representatives from functional business area management, facilities management, and technology management.

6. Custody of the DRP should be the responsibility of a specific individual or group.
7. Contact information for the Disaster Recovery Team members and backup team members must be included in the Plan. Business and non-business hour phone numbers and pager numbers (if available) must be included and should be tested regularly.

Plan activation procedures

1. The Plan must contain detailed instructions and timeframes regarding how to activate and use the DRP.
2. The Plan must contain a schedule of key tasks to be carried out, responsibilities for each task, and a list of services to be recovered, in priority order.
3. Activation procedures should highlight the existence of the wider Business Continuity Plan (BCP) and the DRP's relationship to it.

Hardware and software inventories

1. An inventory of all hardware and software must be included in the Plan. The manufacturer, model, and relevant specifications should be included. All workstations should be included in the inventory.
2. The Information Systems Department management must prepare an annual inventory of production information systems and related network configuration diagrams to facilitate recovery following a disaster. This inventory must indicate all existing production hardware, software, and communications links.

Downtime procedures

1. Procedures to follow when the data center is unable to receive or transmit data must be detailed within the Plan. (Refer to Business Continuity IT Planning Standard for more information concerning department downtime procedures.)
2. User departments must develop adequate manual processing procedures for use until operations are restored.
3. Appropriate departments/individuals should be trained on the DRP and applicable downtime procedures prior to an actual disaster/emergency occurring.

Restoring critical systems, networks, telecommunications

1. The Plan must include detailed instructions for restoring operations (operating systems, critical applications, and networks).
2. Details supporting data retrieval, including retrieval from storage in the event of system interruption and/or disaster, and backup restoration procedures must be included in the Plan.

Hardware restoration and replacement procedures

1. If contractual agreements with third party vendors have been made for hardware replacement, this must be included in the Plan.
2. If there are plans to purchase hardware in the event of a disaster that destroys hardware, these procedures and authorizations with the procurement department must be outlined in the DRP.

Vendor listing

The DRP must contain a list of all vendors, suppliers, and third-party companies that are relied upon to successfully execute the Plan, as well as their role in the execution of the Plan.

Procedures for return to normal operations

1. Determine and document what is required in order to return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the facility will have to operate in the recovery mode.
2. Procedures outlining controlled reentry after emergencies must be included in the Plan.

Off-site storage of Plan

1. Several copies of the current DRP must be stored securely off-site.
2. When updates are made to the DRP, the most recent copy should be sent off-site.
3. The facility should work with the off-site storage provider to ensure the storage provider's continuity plans are appropriate to support the facility's disaster recovery schedule and Plan.
4. Examples include being stored with backup media, in the alternate recovery location, etc.

Alternate Facilities

An "Alternate Facility" is an IT site that can process data and allow business to continue in the event that your facility's local servers and other IT networking hardware are rendered inoperable during a disaster.

1. Alternate locations for recovery must be identified for all primary system locations including HITS, hospital data centers and other areas where in-scope systems are deployed (e.g., PACS systems located in the Radiology department).
2. The Plan must identify the alternate processing facility.
3. The alternative processing facility must be in a state of readiness commensurate with the risks of interrupted operations. The alternate facility readiness significantly impacts the Recovery Time Objectives (RTOs) for critical systems.
4. The alternate processing facility must have sufficient processing capacity and be likely to be available for use. This includes:
   - The ability to support the necessary computer, storage, and network equipment (as well as any ancillary equipment, such as racks) to run the restored systems.
   - This support includes physical space, power, cooling, and connectivity, and should be capable of functioning for weeks or longer depending on the ability to return production systems to the primary location.
5. The alternate processing facility must be geographically removed from the primary processing site.
6. If not a LifePoint location, a contract or inter-facility agreement must be established for the alternate processing facility.
7. If a reciprocal agreement with another facility has been established, consideration must be made for computer, hardware, and telecommunications compatibility with the primary processing site. Options include:
   - Undamaged production IT equipment can be relocated to an alternate site.
   - Recovery equipment is procured and pre-positioned in the alternate site.
   - "Just-in-time" procurement should be pre-arranged for execution after disaster declaration.
8. The contract or inter-facility agreement must include a "right to audit" clause so that the alternate processing facility can be evaluated for its readiness in the event of a disaster.
9. Arrangements for travel and lodging for necessary personnel must be included in the Plan, if needed.

10. Consideration must be taken as to whether production IT equipment may be able to be relocated to the alternate site, if it should be procured and pre-positioned in the alternate site, or if just-in-time procurement should be pre-arranged for execution after disaster declaration.

Testing

1. The DRP must be tested at least annually, and more frequently if there has been a significant change in the facility's data processing environment (such as to network services or legal, regulatory, or contractual obligations).
2. Testing would ideally occur under conditions that simulate a disaster. However, such full-scale tests can be extremely disruptive to facility operations and staff and can also be prohibitively expensive. A reasonable combination of table-top exercises, walk-throughs, and targeted recovery activities that ensure coverage of all key areas is both more realistic and can be conducted more frequently.
3. Test results must be documented, and "lessons learned" must be highlighted.
4. Senior Management must be provided with DRP test results and "lessons learned."

Plan maintenance

1. The DRP must be periodically reviewed and updated to correct any deficiencies identified during testing.
2. The DRP review must tie into the most recent risk assessment to reaffirm recovery priorities.
3. Responsibility for keeping the DRP current must be specifically assigned.

Monitoring

1. The IT Disaster Recovery (DR) Coordinator will monitor (assess) the participation of business owners in the DR process. Any deficiencies in the DRP or deviations from standards that are noted by internal and/or external auditors, or by management will be reported to senior management.
2. LifePoint HITS and other appropriate HSC departments will periodically review the state of the DRP and associated testing at the facilities.
3. Each facility will attest to adherence with this standard in the annual Controlled Self-Assessment.

Responsibility

It is the responsibility of the IT DR Coordinator or designee(s) to implement and maintain compliance with the Business Continuity IT Planning Standard and Disaster Recovery IT Planning Standard.

The following statements are exclusive to the School of Nursing and Allied Health Programs:

Student Personal Information

Once a student provides their personal information to the school, whether it be through the admissions process, financial aid application, health records, etc., the information is securely stored. Electronic information is secured in password-protected databases and information on paper is locked in filing cabinets.

Personally Identifiable information, or PII, is any data that could potentially be used to identify a particular person. Examples include a full name, Social Security number, driver's license number, bank account number, passport number, and email address.

All information that arrives to the Conemaugh School of Nursing and Allied Health Programs is handled securely. A perspective student's initial application is reviewed by either the Admission and Recruitment Chairperson or the Program Director. All applications are kept in a double locked environment. Once accepted, all correspondence that includes personally identifiable information that is on paper or digital is stored securely in either a double locked environment (for paper) or in a secure network folder for digital information. This information includes but is not limited to student applications, references, evaluations, grades, and written classwork or projects.

When transcripts are submitted from another institution they are reviewed and placed in the students' academic file. All academic files are handled securely and maintained permanently in a locked environment. Transcripts that are initiated by the Conemaugh School of Nursing or any Allied Health Program are maintained digitally with either the Administrative Secretary or the Program Director in a secure network folder. After graduation, a permanent paper copy is stored in a secured file.

The school has trained the faculty and staff on the proper handling of PPI and is provided yearly education on cyber security during in-services and Life Talent learning modules. If a topic or incident occurs within the school and is not discussed in this cyber security policy manual then the Hospital policies will prevail.

Financial Aid

Student information is stored on the SON Finance drive. Only the Financial Aid Administrators and the Information Systems Department have access to this drive. This information is maintained and backed up on secure servers by the CMMC Information Systems department.

The Financial Aid Office does not have any authoritative control over these electronic systems. Therefore, the Financial Aid Office complies with all requirements of those parties that house electronic information.

The financial aid department utilizes the following software packages: EdExpress, EdConnect, DirectLoanTools, and an internal Access database system. The financial aid office also uses Department of Education websites that use 2-factor authentication for secure access. These websites include National Student Loan Data System (NSLDS), Common Origination and Disbursement (COD), Pennsylvania Higher Education Assistance Agency (PHEAA) and FAA Access to CPS Online etc.

Financial aid information is kept on a separate share drive. Access to that shared drive is controlled through a request process. On some software (like EdExpress information) the administrator can limit rights within the software. Almost all web-applications require a password and access is granted based on approval from an administrator. For example, many of the Federal Student Aid applications require a universal login. The Primary Destination Point Administrator has to approve the initial requests and then recertify periodically.

Health

All health information that arrives to the Conemaugh School of Nursing and Allied Health Programs is handled securely. Once a student provides their required health information to the school, the information is securely stored. Electronic information is secured in password-protected databases and information on paper is stored and locked in filing cabinets.

Health records are considered confidential. These health records are accessible to the Student Health Nurse and Conemaugh Employee Health Office Medical Director and his/her designee. The Employee Health Office Medical Director and his/her designee may review an accepted student's health records to provide required vaccinations and bloodwork orders for the Student Health Nurse to carry out to meet the CMMC Immunization Guidelines. The Employee Health Office will also store any health records provided to them on a secure password protected database.

Student health information is stored on the SON Health Drive and also the Student Health Office utilizes an internal Access database system. Both of these are password protected. Only the Student Health Nurse and the Information Systems Department have access to this drive. This information is maintained and backed up on secure servers by the CMMC Information Systems Department.

The only time that the Student Health Nurse will share any health information with school administrators, faculty, and staff are if there is a concern for student and/or staff safety in the classroom or in the clinical setting and a need for academic accommodations. A student has the option of disclosing any health information to administrators, faculty, and staff as they choose.

A copy of the health records is stored in a secure file after graduation. At any time, a student or previous student must give written authorization to release any health information and health records. A consent form for Authorization for Release of Protected Health Information may be obtained from the Student Health Nurse. Such information is released to prospective employers, educational institutions, or to the individual requesting the information.

Shred-It

CMMC uses Shred-it for document storage and secure document destruction services. The school retains records according to federal and state regulations and stores on-site when possible. The school utilizes the shredding services of Shred-it to destroy documents with confidential information such as social security numbers, dates of birth, etc. The contact information for Shred-it is as follows:

Shred-it
Phone: (800) 697-4733
www.shredit.com

FERPA

The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA protections go into effect on the first day of classes of the student's first term of enrollment.

FERPA offers students who have attended a post-secondary institution the following rights related to their education records:

- Inspect and review information in their educational records.
- Request a correction to their record.
- Have some control of the disclosure of personally identifiable information from these records (restrict the release of directory information or authorize the disclosure of non-directory information).
- File complaints with the U.S. Department of Education Family Policy Compliance Office (600 Independence Av SW, Washington, DC 20202).

FERPA does not apply to records of applicants for admission who are denied acceptance or, if accepted, do not attend an institution.

Former students have the same FERPA protections regarding their education records; however, they may no longer request that a privacy status be placed on them.

Buckley Amendment

The School of Nursing and Allied Health Programs acknowledges the student's rights to privacy and to review his or her records in compliance with the Family Educational Rights and Privacy Act of 1974, as amended 1976 (Public Law 93-380).

As a result of this Act:

1. Student files are open to the student after a written request is received from the student to the Director, School of Nursing.
2. Records/transcripts/references are released only after written consent is received from the student or graduate.
3. Grades are sent only to the student. The student is responsible for sharing grades with significant others.
4. Conferences with parents, spouse and significant others will be conducted only if the student is present.

Specifically, the student who is over 18 years of age:

1. Is provided with opportunities to privately review grades and evaluations with faculty members.
2. Is able to request a review of grades or evaluations with the Associate Director or Director after review with the appropriate faculty member.
3. May request to inspect and review his or her Educational Record. A written request is made to the Director, School of Nursing office. The student may review the Educational Record at the school's convenience, but within 48 hours of the request. The Record is reviewed in the presence of the Director, School of Nursing, or designee.
4. May not review records for which rights have been waived.
5. May add a written statement to his or her Educational Record.
6. May seek to amend his or her Educational Record.

Records Management

Purpose

Records are maintained by the School of Nursing and Allied Health to serve as a source of historical information.

Confidentiality

Records maintained by the School of Nursing on behalf of its applicants, students, graduates, and employees are retained in a manner which ensures and maintains their confidentiality.

Maintenance

Records retained by the School of Nursing on behalf of its applicants, students, graduates, and program withdrawals are maintained in locked, fire-resistant files under the supervision of the Director, School of Nursing.

- Applicant records are maintained permanently by the Academic Admissions Coordinator/Recruiter.
- Health records are maintained in the office by the Student Health Nurse permanently.
- Financial Aid records are kept in the Office of Financial Aid. (Refer to Financial Aid Policy and Procedure Manual.)

Safety deposit boxes at Ameriserv Financial on Franklin Street store a back-up copy of the graduates' academic transcript and summary of clinical performance (prior to computerization).

Non-permanent records and/or information that exceeds the retention period are disposed of in a manner that ensures confidentiality (i.e., burning, shredding).

Material that is deemed relevant may be added to a specific record at any time. Material that is not relevant to a specific record may be removed and disposed of in a manner that maintains confidentiality.

Custody of Records

The Hospital shall assume responsibility for the safekeeping of all records in the event of closure of the School of Nursing. The Hospital will develop an appropriate procedure for record access and transcript service in the event of school closure. If the Hospital closes, State Board of Nursing advice will be obtained regarding permanent safekeeping and availability of records. The Board shall be notified of record placement.

Access to Records

1. Student academic records are accessible to current faculty members, Director, School of Nursing, the Vice President of Nursing, the Associate Director, the Academic Admissions Coordinator/Recruiter, Financial Aid Administrator, and the school secretaries.
2. Health records are considered confidential, accessible to the Student Health Nurse and Employee Health Office Staff.
3. Financial records are accessible to the Financial Aid, Administration, the Hospital Controller's office, the Associate Director, and the Director of the School.
4. The following persons or organizations may also have access to the student's actual record without his/her consent: State or local officers to whom state law requires information to be reported, organizations such as accrediting agencies, and official representatives of a financial aid source in connection with a student's application for or receipt of financial aid.
5. In compliance with the General Education Act of 1974, as amended in 1976, this school provides the student with the right to inspect his/her own records and to challenge them. A student writes to the Director of the School of Nursing to request a review of the record. If the student believes the record contains inaccurate or misleading information, a meeting is conducted by the Director to evaluate the information. If the meeting does not resolve the conflict, the student may request a meeting with the Vice President of Nursing or a designated institutional official.

6. A student must give written authorization to release information relating to academic and clinical performance. Such information is released only to prospective employers and educational institutions.
7. According to the parents and/or students are transferred to a student who is 18 years of age or is attending an institution of post-secondary education; therefore, permission or consent is required of the student only.
8. Information shall be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the student.

Contents of Records

Student Academic Records are defined as those records for individuals who are currently enrolled in the School of Nursing.

Student records are filed alphabetically by year of expected program completion.

Contents include, but are not limited to:

- Application and submitted reference forms
- Official high school transcript or GED
- Official post-secondary transcripts, if applicable
- Results of pre-admission testing and/or other standardized testing scores, if applicable
- Interview summary
- Acceptance letter
- Right to Know form
- Copies of correspondence between the School of Nursing and the student and/or student and the School of Nursing
- Child Abuse and Criminal Clearance certificates
- Code of Conduct
- Confidentiality form

The student's Conemaugh School of Nursing transcript (academic record) is kept in a separate file during enrollment.

The student's clinical nursing course evaluations and anecdotal records are kept in a separate file during enrollment.

Student Health Records are defined as those records for individuals who are currently enrolled in the School of Nursing. Contents include:

- Student Health record form
- Laboratory testing results

- Cumulative health record
- Other documents as necessitated by the care required for the student during the nursing program
- Health records are maintained in the office by the Student Health Nurse permanently.

Graduate Records are defined as those records maintained for individuals who completed the program and who were awarded a diploma. The complete record at program completion is retained permanently.

In a separate file the Conemaugh School of Nursing academic transcript and "Graduate Summary for Employment" form are retained permanently on hard copy ad infinitum.

The graduate's Health Record (effective since 1995) is retained permanently by the Student Health Nurse.

Inactive Records are defined as those records maintained for individuals who did not complete the program. The entire record is retained permanently.

Contents include any or all of the following:

- Application and submitted reference forms
- Official high school transcript or GED
- Official post-secondary transcripts, if applicable
- Results of pre-admission testing and/or other standardized testing scores
- Interview summary
- Acceptance/rejection letter
- Child Abuse and Criminal Clearance forms
- Code of Conduct
- Right to Know form
- Confidentiality form
- Copies of correspondence between the School of Nursing and the student and/or the student and the School of Nursing
- Academic record (transcript)
- Nursing course evaluations and anecdotal forms

After 5 years, the following contents are retained permanently on hard copy ad infinitum:

- Academic transcript, if applicable
- School of Nursing and the individual's correspondence concerning program detachment, if applicable

Review of Student, Graduate, and Inactive Records

1. The individual may request to review his/her record. A written request is made to the Director of the School of Nursing. Within 48 hours of the request, at the convenience of the Director, the individual may review the record. The record must be reviewed in the presence of the Director, School of Nursing, or designee.
2. The individual may not examine records for which he/she waived rights.
3. The individual may add a written statement to his/her record.

Release of Record Information

1. Personally identifiable information is released only with written consent, except in emergency situations or in connection with financial aid from which the student has applied or received.
2. The student signs a form granting permission for release of information and forms permitting release of grades from Penn Highlands Community College. The forms are signed at registration and are kept in the student's record.
3. Students must sign an Authorization for Release of Protected Health Information.

Release of Academic Record

1. An official transcript is signed by the Director of the School of Nursing and imprinted with the official seal of the Conemaugh Valley Memorial Hospital School of Nursing.
2. An unofficial transcript is not imprinted with the official seal.
3. Transcripts are requested from the Secretary to the Director, School of Nursing, by a written statement signed by the student or graduate.
4. The School of Nursing will release a transcript and/or medical records upon receipt of a written request from the graduate.
5. The envelope containing the official transcript is signed by the Director, School of Nursing, if the official transcript is not sent directly to an agency.
6. The Graduate Summary of Employment is released to agencies requesting a reference for employment after a release is authorized by the student or graduate.
7. Transcripts from other institutions that are part of the student's record may not be sent to a third party.
8. Official transcripts will be released only if all current financial obligations are met.

Preparation of Final Record

Transcripts are compiled, and then signed, by the Director, School of Nursing.

INSTRUCTIONS FOR ACCESSING TRANSCRIPT REQUEST FORM

1. Go to *www.conemaugh.org*

2. Click on Education

3. Click on the specific program attended

4. Click on Transcript Request

5. Fill out appropriate form and return to:

Conemaugh School of Nursing and Allied Health Programs
Attn: Transcript Request
1086 Franklin Street
Johnstown, PA 15905

Exceptions to Student Consent

Per FERPA, there are circumstances under which your education records and personally identifiable information (PII) may be accessed without your consent.

First, the U.S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education or state and local education authorities may allow access to your records and PII without your consent to any third party designated by a federal or state authority to evaluate a federal- or state-supported education program or to researchers performing certain types of studies, even if the university objects to or does not request such research. Federal and state authorities must obtain certain use-restriction and data security promises from the entities that they authorize to receive your PII, but the authorities need not maintain direct control over such entities.

In addition, in connection with Statewide Longitudinal Data Systems, state authorities may collect, compile, permanently retain and share without your consent PII from your education records, and they may track your participation in education and other programs by linking such PII to other personal information about you that they obtain from other federal or state data sources, including workforce development, unemployment insurance, child welfare, juvenile justice, military service and migrant student records systems.

FERPA allows the institution the right to disclose education records or identifiable information to individuals/entities without the student's consent under the following circumstances:

- Authorized representatives for audit of federal- or state-supported programs.
- University officials carry out their specifically assigned educational or administrative responsibilities. This includes contractors, consultants, volunteers, and other outside providers used by the University of Colorado Boulder, including the University of Colorado Foundation and the National Student Clearinghouse.
- Veteran's Administration officials.
- Officials of other institutions at which a student seeks or intends to enroll.
- Persons or organizations providing financial aid to students.
- Organizations conducting studies for, or on behalf of, educational agencies or institutions to develop, validate and administer predictive tests, to administer student aid programs or to improve instruction, provided that individual identity of students is not made.
- Accrediting organizations carrying out their accrediting functions.

- Parents of a student who have established that student's status as a dependent according to Internal Revenue Code of 1954, Section 152; in connection with a health and safety emergency in connection with § 99.36; or the student is under 21 and has violated a federal, state or local law or a policy of the university related to the use or possession of alcohol or a controlled substance.
- Persons in compliance with a judicial order or a lawfully issued subpoena, provided that the institution makes a reasonable attempt to notify the student in advance of compliance. The institution is not required to notify the student if a federal grand jury subpoena, or any other subpoena issued for a law enforcement purpose, orders the institution not to disclose the existence or contents of the subpoena.
- Persons in an emergency, if the knowledge of information, in fact, is necessary to protect the health or safety of students or other persons.
- An alleged victim of a crime of violence of the results of any institutional disciplinary proceeding against the alleged perpetrator. Information may only be given in respect to the crime committed.
- Outside contractor when identified as a "party acting for" the institution and performing a service which the institution would otherwise have to perform for itself (for example, the National Student Loan Clearinghouse for loan verification).
- Representatives of the Department of Homeland Security or Immigration and Customs Enforcement, for purposes of the coordinated interagency partnership regulating the Student and Exchange Visitor Information System (SEVIS).
- The attorney general of the United States or the attorney general's designee in response to an *ex parte* order in connection with the investigation or prosecution of terrorism crimes, under the US Patriot Act.
- In addition, FERPA allows the following:

- The return of an education record, or information from an education record to the party identified as the provider or creator of the record.
- The release of education record and PII information regarding a registered sex offender's enrollment or employment status, or any changes of such.
- The release of education record and PII information to appropriate parties if the school determines that there is an articulable and significant threat to the health and safety to a student or other individuals.

Release of Disciplinary Information

Provisions of FERPA, as amended by the Higher Education Amendments of 1998, govern access to a student's disciplinary file. The student and/or university officials who demonstrate a legitimate educational need for disciplinary information may have access to the student's disciplinary file. Parent(s) can have access to the student's disciplinary file without written consent of the student even if the student has requested otherwise.

In addition, parent(s) may be notified if a student under 21 years of age is found responsible for a violation involving use or possession of alcohol and drugs.

The Campus Security Act permits higher education institutions to disclose to alleged victims of any crime of violence (murder, robbery, aggravated assault, burglary, motor vehicle theft) the results of the conduct proceedings conducted by the institution against an alleged perpetrator with respect to such crime. The Campus Security Act also requires that both accused and the accuser be informed of campus conduct proceedings involving a sexual assault.

Additionally, institutions are permitted to disclose the results of disciplinary cases in which a student has been found responsible for a violation involving violence or for a sex offense.

Pennsylvania Statutes

Title 73: Trade and Commerce

Chapter 43: Breach of Personal Information Notification Act

Effective: June 20, 2006

§ 2301. Short title. This act shall be known and may be cited as the Breach of Personal

Information Notification Act.

§ 2302. Definitions. The following words and phrases when used in this act shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Breach of the security of the system." The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the purposes of the entity is not a breach of the security of the system if the personal information is not used for a purpose other than the lawful purpose of the entity and is not subject to further unauthorized disclosure.

"Business." A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this Commonwealth, any other state, the United States or any other country, or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records.

"Encryption." The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"Entity." A State agency, a political subdivision of the Commonwealth or an individual or a business doing business in this Commonwealth.

"Individual." A natural person.

"Notice." May be provided by any of the following methods of notification:

1. Written notice to the last known home address for the individual.
2. Telephonic notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
3. E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.
4. Substitute notice if the entity demonstrates one of the following:
   a. The cost of providing notice would exceed $100,000.
   b. The affected class of subject persons to be notified exceeds 175,000.
   c. The entity does not have sufficient contact information.

   Substitute notice shall consist of all of the following:

   a. E-mail notice when the entity has an e-mail address for the subject persons.
   b. Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.
   c. Notification to major statewide media.

"Personal information.”

1. An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:
   a. Social Security number.
   b. Driver's license number or a state identification card number issued in lieu of a driver's license.
   c. Financial account number, credit, or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
2. The term does not include publicly available information that is lawfully made available to the general public from Federal, State, or local government records.

"Records." Any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted. The term does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, such as name, address, or telephone number.

"Redact." The term includes, but is not limited to, alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data.

"State agency." Any agency, board, commission, authority or department of the Commonwealth and the General Assembly.

§ 2303. General rule.

(a) General rule.--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 [FN1] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored, or managed by the entity, is in this Commonwealth.

(b) Encrypted information.--An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

(c) Vendor notification.--A vendor that maintains, stores, or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores, or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

§ 2304. Exceptions. The notification required by this act may be delayed if a law enforcement agency determines and advises the entity in writing specifically referencing this section that the notification will impede a criminal or civil investigation. The notification required by this act shall be made after the law enforcement agency determines that it will not compromise the investigation or national or homeland security.

§ 2305. Notification to Consumer Reporting Agencies. When an entity provides notification under this act to more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

§ 2306. Preemption. This act deals with subject matter that is of Statewide concern, and it is the

intent of the General Assembly that this act shall supersede and preempt all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities, and other local agencies within this Commonwealth regarding the matters expressly set forth in this act.

§ 2307. Notice exemption.

(a) Information privacy or security policy.--An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and is consistent with the notice requirements of this act shall be deemed to be in compliance with the notification requirements of this act if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(b) Compliance with Federal requirements.--

1. A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this act.
2. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional Federal regulator shall be in compliance with this act.

§ 2308. Civil relief. A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L. 1224, No. 387), known as the Unfair Trade Practices and

Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

§ 2329. Applicability. This act shall apply to the discovery or notification of a breach in the security of personal information data that occurs on or after the effective date of this section.

APPENDIX A: INFORMATION CONFIDENTIALITY & SECURITY AGREEMENT

Conemaugh Health System

Confidentiality and Security Agreement

I understand that the Conemaugh Health System (CHS), in which or for whom I work, volunteer or provide services, or with whom the entity (e.g., physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of CHS' health information, has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, CHS must assure the confidentiality of its information that relates to its employees and technological activities; medical and scientific research; business activities, including marketing of services and recruiting staff and employees, business plans, purchasing, accounting, data processing or management information systems; licensing of patents, trademarks or service marks and copyrights; and all other information or material that Conemaugh Health System considers confidential or a "trade secret" as that term is used in the law. All such information or material is referred to collectively as "Confidential Information" in this Agreement).

In the course of my employment / assignment at CHS, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job-related duties in accordance with the Conemaugh Health System Privacy and Security Policies, which are available on the CHS intranet. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.

2. I will only access software systems to review patient or other information when necessary to perform my job duties

3. I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized

4. I will not discuss Confidential Information where others can overhear the conversation. It is not acceptable to discuss Confidential Information even if the patient's name is not used.

5. I will not make any unauthorized transmissions, inquiries, modifications, or purgings of Confidential Information.

6. I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with CHS.

7. Upon termination, I will immediately return any documents or media containing Confidential Information to CHS.

8. I understand that I have no right to any ownership interest in any CHS information accessed or created by me during my relationship with CHS (except where explicitly permitted).

9. I will act in the best interest of CHS and in accordance with its Code of Conduct at all times during my relationship with CHS.

10. I understand that violation of the Agreement may result in disciplinary action, up to and including termination of employment, suspension, and loss of privileges, and/or termination of authorization to work within CHS, in accordance with CHS policies. I understand that legal action may be taken against me depending on the violation's severity.

11. I will only access or use systems or devices I am officially authorized to access and will not demonstrate the operation or function of systems or devices to unauthorized individuals.

12. I understand that I should have no expectation of privacy when using CHS information systems. CHS may log, access, review, and otherwise utilize information stored on or passing through its systems including e-mail, in order to manage systems and enforce security.

13. I will practice good workstation security measures such as locking up diskettes when not in use, logging out of applications containing sensitive information when leaving the workstation unattended, and positioning screens away from public view.

14. I will practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards and procedures.

15. I will:
    a. Use only my officially assigned User-ID and password.
    b. Use only approved licensed software.
    c. Use a device with virus protection software.

16. I will never:
    a. Share/disclose user-Ids or passwords.
    b. Use tools or techniques to break/exploit security measures.
    c. Connect to unauthorized networks through the systems or devices.

17. I will notify my manager, Security Coordinator, or appropriate MIS person or system administrator if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.

The following statements apply to physicians using CHS systems containing patient identifiable health information (e.g., Care Portal):

18. I will only access software systems to review patient records when I have that patient's authorization to do so, or if I am involved in the patient's current episode of care. By accessing a patient's record, I am affirmatively representing at the time of each access that I have the requisite patient authorization to do so or I am involved in the current episode of care, and CHS may rely on that representation in granting such access to me.

19. I will ensure that only appropriate personnel in my office will access CHS' software systems and Confidential Information and I will annually train such personnel on issues related to patient confidentiality and access.

20. I will accept full responsibility for the actions of my employees who may access CHS software systems and Confidential Information.

Signing this document, I acknowledge that I have read this Agreement and I agree to comply with all the terms and conditions stated above.

Printed Name: **ACTUAL FORM LOCATED ON CHS INTRANET PAGE**	Date:
Signature:	Employee/Badge #: (if applicable)
Company Name/Address: (if applicable)	

Appendix B

Conemaugh Memorial Medical Center

EMERGENCY RESPONSE PROGRAM

Cyber Incident Response
2024

Cyber Incident Response Team - Emergency Response Program (Hospital Team)

LifePoint Health, Inc. (the “Company”) is committed to being prepared to respond to a cyber incident that could impact the Company’s operations. This Hospital Emergency Response Program (ERP) is intended to provide guidance to the Company’s personnel responding to such an event. This ERP will be implemented for any Company cyber event that impacts operations due to a cyber event or ransomware.

An important part of any ERP is that the scale of the program is appropriate to the size and scope of the operation. This document describes the Hospital’s ERP and the overall response strategy and provides guidance on initial steps to be taken to activate the program. All incident response actions will be aligned with the Company’s designated escalation process, summarized below:

Step 1 Hospital Support Center(“HSC”) Information Security-identified security incident or Hospital IT / Leadership Team report security incident to HSC Information Security. Reports can be communicated through the Company’s 24x7 ServiceDesk indicating a critical incident that needs HSC Information Security support.

Step 2 HSC Legal, HSC Compliance, and HSC Information Security (the “Compromise Assessment Team”) meet to understand cyber incident impact to operations and determine whether ransomware is involved. The Compromise Assessment Team will be the primary governance body as the cyber event progresses.

Step 3 HSC Legal appoints outside counsel to assist with response efforts. In choosing outside counsel, HSC Legal shall coordinate with HSC Risk, as needed, to select a counsel that has been or will be approved by cyber liability insurance provider.

Step 4 HSC Information Security will set up Microsoft Teams call bridge to provide update to the appropriate Hospital Leadership Team and appropriate Divisional Leadership Team on operational impacts due to ransomware or cyber event.

Step 5 Professionally manage response efforts to reduce impact to patient care, the facility, and operations.

Step 6 Determine what occurred and modify procedures as necessary to attempt to prevent recurrence.

Program Distribution

The Hospital ERP is carried out by Key Responders. These Key Responders include:
Hospital Leadership Team

CEO	Rodney Reiter
CFO	Lynn Kennington
COO	na
CIO / HDIS	Nate Defanti \Brian Belz
Facility Privacy Officer	Lauren Ashcom Chapman (Compliance Officer) Brian Belz (FISO)
Administrative Support	(To be determined at time of response)

HSC Key Responders

Divisional Leadership Team	
Division Communications	
HSC CIO	(Alan Smith)
HSC CISO	(Andy Heins)
AVP, Cyber Defense Mgmt.	(John Beauchamp)
Chief Privacy Officer	(Tizgel High)
Deputy General Counsel	(Fabio Fallico)

Functional responsibilities for each Key Responder are outlined below in this ERP.

Organization and Responsibilities

The HSC will establish direction and control for the entire response and will act as the strategic decision-making body to respond to internal and external demands.

Notification and Verification of an Event

Initial notification may come as a telephone call or electronic notifications to the HSC Information Security Team (Cyber Defense Management) monitoring or by other means. Upon receipt of initial notification and confirmation of potential threat, the recipient shall immediately notify the Compromise Assessment Team (HSC Legal, HSC Compliance, and HSC Information Security) to evaluate threat. The CISO will coordinate a conference call with the Executive Leadership Team. If the Company's CISO is unavailable, the CIO will assume responsibility for the Company's overall response.

Incident response begins with verification that the facility or hospital has been involved in a cyber event that has impacted the Company. Verification consists of the HSC Cyber Defense Management Team being contacted or contacting the Hospital IT Leadership and Hospital Leadership Team. Upon verification that an event involves a technology operational disruption or ransomware, this ERP will be implemented as described below.

Implementation of ERP

Notification of HSC Key Responders and Initial Brief

After verification of a cyber event has occurred, CISO will assemble the HSC Key Responder group. The CISO or CIO will inform the group what is known and assign roles and responsibilities to respond to the event. This briefing will be fact based, and personnel assignments will be made based on who is available.

Upon completion of this initial brief, HSC Key Responders will immediately implement the balance of this ERP with continued engagement with the Hospital Leadership Team.

As staff is available, personnel will be scheduled in shifts to cover responses requiring a 24-hour presence. This is a highly stressful environment, which may last several days. If sufficient staff is available, more than one person who can fill each position will be assigned to allow for rest periods. Other Health Information Technology Services ("HITS") departments or third-party resources may fill in as needed to continue to the response efforts.

Notification of Company Insurance Carriers

In coordination with outside counsel, the Senior Vice-President of Risk Management will coordinate notification of the Company's insurer carrier.

Notification of LifePoint Health Personnel and Media

The HSC Communications Department will coordinate communication of the event to Company personnel at a time and in a manner to be determined by HSC Communications, with outside counsel's assistance, as well as from the assigned public relations communication firm. The HSC Communications Department will also coordinate the Company's response for all media requests for information.

Notification of Law Enforcement

The HSC Legal Department will coordinate all written notifications with outside counsel. After consultation between the HSC Legal Department and the HSC CIO, either the HSC Legal Department or outside counsel will coordinate initial verbal contact with Law Enforcement from the Federal Bureau of Investigation, United States Secret Service or other applicable law enforcement. Contact information can be found in the Data Event Response Plan Guideline.

Key Responder Responsibilities

Functional responsibilities for each Key Responder are outlined as follows:

HSC ELT Member (may include both Division Leadership Team and Hospital Leadership Team)

a. Coordinate with HSC Communications and outside counsel on appropriate internal and external communication on talking points and holding statements;
b. In coordination with outside counsel, verbally notify internal stakeholders of incident (Apollo Global Management, Board of Directors, Joint Venture Partnerships, etc.); and
c. Coordinate with HSC Communications and outside counsel on appropriate communication on holding statements for external stakeholders, company, public website, and media.

HSC Risk Management

a. Notify Cyber insurance carrier per insurance policy terms;
b. If applicable, coordination of Call Center if applicable for disclosure / patient notification; and
c. If applicable, coordinate identity protection / credit monitoring services.

HSC Communications (may include Division Communications)

a. In coordination with outside counsel, notify public relations communications firm and breach coach;
b. In coordination with outside counsel, prepare initial internal statement from the Company;
c. Determine whether on-site media representative will be assigned and arrange transportation;
d. Define Social Media Management Plan; and
e. Perform Notification of media (newspapers, websites, etc.) based on reporting obligations.

HSC Information Security – Cyber Defense Management (includes Hospital CIO / HDIS)

a. Coordinate HSC Event Response Team Conference Line and triage updates to ELT;
b. Coordinate HITS response and mitigation efforts; pull in other HITS teams, as necessary;
c. In collaboration with outside counsel, coordinate efforts of third-party cyber security companies (i.e., MSSP, CrowdStrike);
d. Coordinate forensic information from endpoint detection response technologies and managed security services companies;
e. Coordinate Hospital Communication Call Bridge to communicate status with Hospital IT Leadership and Hospital Leadership Teams; and
f. Coordinate with third-party service providers (e.g., CereCore) as necessary.

HSC Legal

a. Engage the Company's outside counsel for assistance in complying with statutes and regulations related to the event. Counsel has been approved by cybersecurity insurance provider:

Bass Berry and Sims, PLC
ATTN: Robert Brewer, Member
Cell: 615-500-2806

b. Engage additional resources, as necessary, to ensure the Company's compliance with legal standards;
c. Through outside counsel, engage cyber security forensic company to perform investigation;
d. Engage ransomware professional services negotiator, if applicable; and
e. Perform Credit Card Investigation (if appropriate) through cyber security forensic company.

HSC Compliance / Privacy (include Facility Privacy Officer)

a. Coordinate with HSC Compliance on four Factor Risk Assessment / Notification to OCR / HHS Website legal requirements; and
b. Coordinate with outside counsel if federal or state notification requirements must be met.

HSC HITS (include Hospital CIO / HDIS)

a. Evaluate technology operational response resources to assist impacted operations recover if devices have been impacted with ransomware;
b. Coordinate remediation response with third-party vendors or network service providers;
c. Assist in system shut down and recovery as necessary; and
d. Assist in obtaining additional outside resources (as needed) to help with remediation efforts.

HSC Human Resources

a. If members of the event response team need to travel to a location operationally impacted, evaluate if Company aviation team can assist with travel arrangements if commercial flight options are not available; and
b. In the event post forensic report determines employee data is impacted, coordinate with outside counsel, HSC Communications on internal communications.