Penn Medicine
Lancaster General Health

POLICY TITLE: Safeguarding Confidential Information
Former Policy Title:

POLICY PURPOSE:

The purpose of this policy is to establish safeguards that protect confidential information from unauthorized access, use or disclosure and to further protect such information from tampering, loss, alteration, and/or damage while in transit or at rest.

POLICY STATEMENT:

Lancaster General Health (LG Health) will implement appropriate and reasonable administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of confidential information. LG Health will use protections that are flexible, scalable, and provide reasonable safeguards. The safeguards implemented may vary depending on factors such as the size, location and/or nature of its business.

LG Health will take into consideration the potential impacts on patient care and other issues such as the financial and administrative burdens of implementing various safeguards.

Confidentiality Agreements will be signed by workforce and non-workforce members, as indicated.

- **Confidentiality and Access Agreement** – all workforce and non-workforce members requiring access to electronic resources and/or information systems. See appendix A.

- **Confidentiality Agreement for Non-Workforce** – non-workforce members who may have access to confidential information as a result of their activity at LG Health, but do not require a User ID and Password to electronic resources (e.g., Tours, Shadowing, and Site Visits). See Appendix B.

APPLICABILITY/SCOPE/EXCLUSION:

The policy is applicable to all LG Health business units and departments that maintain confidential information. The scope of confidential information to be safeguarded is regardless of medium or form by which it is communicated or maintained (electronic, verbal, paper, etc.).

DEFINITIONS:

Confidential Information: Protected Health Information (PHI), certain financial records including credit card information, human resources, payroll, and all other information classified as confidential.

POLICY TITLE: SAFEGUARDING CONFIDENTIAL INFORMATION

Workforce: Employees, members of the Medical and Dental Staff, volunteers, trainees, and other persons whose conduct, in the performance of their work for LG Health, is under the direct control of LG Health, regardless of whether they are compensated by the organization.

Non-Workforce: Individuals who do not meet the definition of Workforce (above). Examples include individuals on a site visit, on tour, or job shadowing without access to information systems.

PROCEDURE:

Paper - Each department will maintain confidential files and documents in locked rooms, lockable desks, or lockable storage systems.

- If a patient care area is staffed 24/7/365 **and** it is not reasonable or practical to lock the confidential information because of the impact to patient care, the area will take reasonable precautions to ensure that confidential information is protected from unauthorized access or disclosure. For example, keep confidential documents out of arms reach, face down, or otherwise concealed.

- Shredding, disposing, or otherwise destroying confidential files or documents shall be consistent with the Waste Management, Disposal, and Recycling Policy, Appendix G Recycling/Disposal of Confidential Information.

- Special care should be used when providing copies of documents to patients or authorized requesters of information to ensure only documents relating to the request are provided. This will prevent documents being provided to the incorrect recipient (see policy entitled "Identity Verification").

- Remove confidential information from print/copier/fax devices as soon as possible.

- Do not remove confidential information from work locations unless specifically authorized.

- When authorized to transport paper containing confidential information the paper will be safeguarded from incidental or unauthorized access by the use of envelopes for internal mail, locked bags for transport, or other controls to protect the information.

- Do not use postcards to communicate patient-specific information.

- Limit the use of return addresses or logos that identify a diagnosis/procedure specific location when mailing a patient regarding their care.

Electronic -

- Do not save confidential information to a local drive (C: drive) on a computer; only save confidential information to shared drives or other authorized locations to ensure the data is protected from device theft or loss.

- Restricted and Sensitive data should not be stored or accessed on personal services or devices, except if a user has agreed to have the personal mobile device managed using Penn Medicine Mobile Device Management and it is enabled, in which case restricted data may be used on a personal mobile device (see Penn Medicine Information Security Policy and Standard entitled "Data Classification Policy" and "Information Handling Standard").

- All LG Health data stored on removable electronic media will be stored only on approved storage devices (e.g., encrypted USB flash drive).*

  *NOTE – LG Health will honor patient requests to obtain or transmit their health information in an unsecured format

Verbal: Although preventing incidental disclosures of all confidential information is not possible in some patient care settings, discussions with patients and families should be conducted as discreetly as possible to minimize the incidental disclosures. In non-patient care or public settings, confidential information should not be able to be overheard by others in the area. (See policy entitled "Disclosures of Protected Health Information to Family and Friends."

Telephone: Departments shall develop specific guidelines for communicating confidential information via the telephone, including process for positive identification of the caller, as appropriate for their business needs.

Visual: Confidential information will be adequately protected from unauthorized disclosure on computer monitors and whiteboards.

Faxing: The location of fax equipment must be in a secure, non-public area. A fax cover sheet must accompany all fax transmissions of confidential information. Note: Point of Care documents faxed internally do not require a cover page.

Required elements of a fax cover page

- Penn Medicine Lancaster General Health name and address
- Sender's name and telephone number
- Recipient's name and fax number
- Date and time of the fax transmission
- Number of pages transmitted (including the cover letter)
- Disclaimer Statement as follows:

  The document(s) accompanying this fax transmission contain information from Penn Medicine Lancaster General Health which may be confidential and/or legally privileged. This information is intended only for the use of the individual or entity named on this transmission sheet. The authorized recipient of this information is prohibited from disclosing this information to any other party without the authorization of Lancaster General Health. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this fax transmission in error, please notify us by telephone immediately at the above telephone number so that we can arrange for the return or destruction of these documents.

Additional/optional elements of a fax cover page include the Sender's fax number and the Recipient's telephone number.

Routine faxed numbers will be pre-programmed into fax equipment and fax information systems to eliminate misdirected dialing. Staff will perform verification of pre-programmed fax numbers routinely by using or verifying the fax number entered into the system.

ROLES/RESPONSIBILITIES:

The Health Information Management Department will oversee, develop and implement procedures specific to the disclosure of protected health information (PHI) pursuant to an official request or patient authorization (See policies entitled: "Disclosures of Protected Health Information with Patient Authorization", "Disclosures Where No Form of Patient Permission is Required Policies", Uses and Disclosures of PHI for Treatment, Payment and Healthcare Operations" "Access to Protected Health Information by Personal Representatives", "Disclosures of Protected Health Information to Family and Friends" and "Patient's Right to Access, Inspect or Copy Their Protected Health Information."

APPENDICES:

Safeguarding Confidential Information – Appendix A - Confidentiality and Access Agreement
Safeguarding Confidential Information – Appendix B - Confidentiality Agreement for Non-Workforce

FORMS: N/A

REFERENCE DOCUMENTS:

Access to Protected Health Information by Personal Representatives
Disclosures of Protected Health Information to Family and Friends
Disclosures of Protected Health Information with Patient Authorization
Disclosures Where No Form of Patient Permission is Required
Identity Verification
Patient's Right to Access, Inspect or Copy Their Protected Health Information
Uses and Disclosures of PHI for Treatment, Payment and Healthcare Operations
Waste Management, Disposal, and Recycling Policy
Penn Medicine Information Security Policy – Data Classification
Penn Medicine IS Security Standard – Information Handling
Penn Medicine IS Security Standard – Electronic Media, USB Drive Standard
Penn Medicine IS Security Standard – Email Management Standard
Penn Medicine IS Security Standard – Mobile Device Security Standard