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.

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.

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:

Workforce members must implement reasonable safeguards to minimize the risk of unauthorized access, use and disclosure of Confidential Information. Reasonable safeguards include, but are not limited to:

General:

- Accessing and using confidential information only as necessary to perform one's job functions.

- Sharing confidential information with requesters only after verifying their identity and their authority to access the information (see policy entitled "Identity Verification").

- Sharing only documents covered by the authorized request when authorized to share confidential information with requestors of information.

- Ensuring that workforce members and non-workforce members sign applicable confidentiality statements.

Paper:

- Maintaining confidential files and documents in locked rooms, lockable desks, or lockable storage systems. If this is not feasible, using other methods to protect from unauthorized access, such as keeping documents face down or hard to reach.

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

- Removing confidential information from print/copier/fax devices as soon as practicable.

- Removing confidential information from work locations only when specifically authorized.

- When transporting documents containing confidential information, using envelopes for internal mail, locked bags for transport, or other controls to protect the information.

- When working from home, limiting printing to what is necessary, keeping documents organized and in one place, avoiding leaving confidential information in readily accessible locations and when possible, storing documents in a locked cabinet or storage box.

- In mailings, limiting the use of logos or other information that indicates a diagnosis or procedure related to a patient.

Electronic: See University of Pennsylvania Health System (UPHS) Information Security policies for a complete list of electronic safeguards.

- Avoiding leaving portable computing devices unattended in public areas.

- Avoiding saving confidential information on local drives or personal devices, unless they are managed by Penn Medicine Information Services.

- Keeping passwords secure and private. Sharing of passwords is prohibited. Further, any prohibited behavior that takes place under user credentials is considered to be done by that user.

- Locking computer screens on workstations when user is not using such workstations.

- Sending sensitive information only to recipients who is not authorized to receive it.

- Sending sensitive information to an authorized recipient using reasonable methods to secure it in transit or transmission.

- Not auto-forwarding email – auto-forwarding email is prohibited.

- When disposing of computer devices, using reasonable methods to ensure sensitive data residing on it is securely destroyed and any further access to sensitive data is disabled.

- Storing Confidential information only:
    - Institutionally secured and managed network drive
    - Institutionally secured and managed encrypted device
    - Institutionally approved third-party computing environment (see UPHS Information Security Policy entitled "Data Protection Policy".

Verbal

- Avoiding speaking in a loud voice or otherwise being overheard by unauthorized individuals.

E-mail:

- When possible, avoiding transmitting confidential information in email because of risks associated with email. If email must be used to transmit PHI:
    - Use Penn Medicine's email system.
    - Limit PHI and identifiers to the minimum amount needed to achieve the purpose of the communication, without compromising patient safety.
    - Use [encrypt] anywhere in the subject line force encryption.
    - Do not use publicly available email systems like Gmail and Yahoo, for business communications. Auto-forwarding of Penn Medicine email to external or personal mail accounts is also not permitted.

- In all cases, avoiding using email to send:
    - highly sensitive information (such as social security numbers, diagnoses, and treatment for certain specially-protected conditions such as mental health, substance abuse, and HIV information);
    - documents containing information about numerous individuals (such as schedule lists for specific procedures or spreadsheets of data used in research or other analysis or business operations); and
    - information that directly or indirectly reveals patient PHI to groups of recipients, such as listservs of patient names or research subjects.

- As alternatives to email, using entity-approved file-sharing systems and shared drives, as well as messaging within the patient portal and electronic medical records systems.

Faxing

- Locating fax equipment in a secure, non-public area.

- Verifying pre-programmed fax numbers periodically and routinely.

- Ensuring that a fax cover sheet, containing language that the information is intended for the named recipient and if received by someone else to contact Penn Medicine to mitigate privacy risks, accompanies 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.

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:

LG Health Policy -Waste Management, Disposal, and Recycling Policy
Penn Medicine Information Security Policy – Acceptable Use of Information Resources
Penn Medicine Information Security Policy – Data Classification
Penn Medicine Information Security Policy – Data Protection

Penn Medicine IS Security Standard – Electronic Media, USB Drive Standard
Penn Medicine IS Security Standard – Email Management Standard
Penn Medicine IS Security Standard – Information Handling
UPHS HIPAA Policy -Identity Verification

Penn Medicine
Lancaster General Health

CONFIDENTIALITY AND ACCESS AGREEMENT

Lancaster General Health (LG Health) recognizes that you may have access to confidential information including, but not limited to, patient records (including patient demographic information), financial records, and personnel or other business-related information, either directly or indirectly (together, "Confidential Information"). All types of Confidential Information must be protected. As a condition to being granted access to Confidential Information, you agree to:

1. **Only** access Confidential Information on a need-to-know basis to perform your job duties or fulfill your contractual obligations.
2. **Never** access Confidential Information out of curiosity or non-business-related reasons. By way of example only, unless you have a business need to do so, you must not access records relating to the following:
   - Your immediate or extended family members (for example, your spouse or children),
   - Your friends, significant others, co-workers,
   - People in the news (for example, accident victims or famous people).

NOTE: Accessing your own electronic health record out of curiosity or for non-business-related reasons is outside the performance of your job duties and, therefore is **prohibited**.

   - To request access to your own health record, contact Medical Records Services (717-544-5913).
   - You can also access and manage your own records online through your own personal MyLGHealth account.

3. **Protect** Confidential Information by:
   - Logging off or locking the computer before you walk away from it
   - Encrypting any mobile device (for example, a smart phone, tablet, laptop, or USB drive) that has Confidential Information on it
   - Not leaving Confidential Information or mobile devices containing Confidential information unattended or within public access or view
   - Not leaving Confidential Information unattended or within public access/view – including paper, computers, mobile devices, etc.
4. **Never** share your password with anyone.
5. **Immediately** report confirmed or suspected privacy or security concerns or violations (see below for reporting methods).

Also, as a condition to being granted access to any Confidential Information, you acknowledge and understand that:

- All forms of Confidential Information must be protected, including written, electronic, oral, overheard or observed. Patient information must be treated as confidential in accordance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and any other state or federal law that may apply.
- You are prohibited from removing, retaining, disclosing, using or sharing Confidential Information after you are no longer working for or affiliated with LG Health.
- Your user ID and password is your electronic signature and is treated as your written signature with all legal implications.
- You are responsible for any action taken or documentation made when you are logged into a system or application with your user ID.
- Your access to LG Health systems and its content (for example email) may be checked from time to time by LG Health.
- If you do not comply with this Agreement, you will be subject to immediate corrective action, up to and including termination of your access to LG Health electronic systems and/or your employment or affiliation with LG Health, if applicable.
- If your access, employment and/or affiliation are terminated for violations of this Agreement, you may not be allowed access to LG Health information systems even if you become employed by another health care provider or company.

NOTES: All workforce members must follow all other LG Health policies and procedures relating to accessing electronic systems. LG Health workforce includes, but is not limited to, employees, medical staff, students, faculty, volunteers, temporary personnel, and other persons under the direction of LG Health, whether or not they are paid by LG Health.

Consultants/Contractors/Vendors may also be obligated to additional requirements above and beyond this Agreement based upon a specific contractual agreement with LG Health.

Please complete the following:

Name of Employer/Organization/Company	Your Department and/or Position Title
Immediate Supervisor's Name (if applicable)	Last 4 Digits of Social Security *(required for password reset identity validation)* XXX – XX – _____

By signing this below, I indicate that I have read and understand the above terms and conditions, and that I voluntarily accept them and agree to abide by them.

Signature _____ Date _____

Full Legal Name (please print) _____

* *(For Consultant/Contractor/Vendor Use Only)* *

Company Name (printed) _____ Date _____

Start Date: _____ End Date: _____

LGHA-9468 7/19R

To report information security or privacy violations or concerns to the Entity Privacy Officer you can email Privacy@LGHealth.org, call 717-544-4060, or call anonymously Compliance Alertline at 1-888-411-3380.

Penn Medicine
Lancaster General Health

Confidentiality Agreement for Non-Workforce

I,_____, will be engaging in the following activity:

_Tour _Shadowing Activity _Site Visit

As a condition of engaging in that activity, I agree to the terms and conditions described below.

As part of my activity here at Lancaster General Health (LG Health), I may have access to LG Health confidential information such as patient records, financial records, and personnel or other business-related information, either directly or indirectly (together, "Confidential Information"). All types of Confidential Information must be protected. This includes information that is written, electronic, spoken, overheard, or observed.

Because I may have access to Confidential Information, I agree to the following:

I Will:

- Treat any patient information as confidential, following the Health Insurance Portability and Protection Act of 1996 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and any other state or federal law that may apply.
- Protect the privacy of all Confidential Information during my activity at LG Health and after I leave.

I Will Not:

- Disclose, communicate, reproduce, sell, copy, post on social media, post on the Internet, or otherwise make public or share any Confidential Information with any other entity or person, including family, friends, significant others, co-workers, or anyone else, except as required by law.

I Understand:

- If I disclose or misuse Confidential Information, my activity may be ended.
- If I disclose Confidential Information without authorization to do so, it may be harmful to the patient or LG Health. If this would happen, the patient or LG Health may have the right to take legal action against me.
- LG Health may end my activity or remove me from its facilities for the following reasons (at its discretion and at any time):
  a. Unacceptable conduct, attitude, attire, and/or lack of cooperation.
  b. Violation of any instructions or any policies or rules that have been shared with me that apply to my activity.
- The use of photography, video, and sound equipment is not permitted.
- I am not, will not be considered to be, and will not represent myself as an employee of LG Health or any of its affiliates as a result of my participation in the activity listed above. I am not entitled to payment or benefits of any kind from LG Health for my participation in this activity.

I Will Follow These Guidelines:

- If requested, an ID Badge must be worn at all times while in any LG Health facility.
- Food or drinks are allowed only in designated areas.

By signing below, I indicate that I have read the above terms and conditions and that I voluntarily accept them and agree to abide by them.

_____ _____
Signature Date

_____ _____
Printed Name Company Name (if applicable)

_____ _____
Parent/Guardian Co-Signature (required for individuals under the age of 18) Date

(For staff use only)

Staff Member Name (printed)_____

Title: _____ Department:_____