Issuing Department: Internal Audit, Compliance, and Enterprise Risk Management

Effective/Reissue Date: 10/5/2016
Current Version: 7/1/2022

Safeguarding PHI

Policy

NYU Langone Health will use reasonable and appropriate administrative, technical, and physical safeguards to limit intentional or unintentional Uses and Disclosures of Protected Health Information ("PHI"). NYU Langone Health will also use these safeguards to protect against the inadvertent Disclosure of PHI to persons other than the intended recipient.

Workforce Members will only access PHI when there is a legitimate clinical, billing, or business reason to do so. NYU Langone Health will monitor all information systems, networks, hardware, and NYU Langone Health work sites to ensure compliance with this Policy.

Procedures

Administrative, technical, and physical safeguards include but are not limited to the following procedures:

1. All Workforce Members are required to read and sign the *Privacy, Information Security, and Confidentiality Statement*. This form will be retained in the individual's Human Resources file or where otherwise applicable.

2. Protecting Oral PHI:
    - Conversations in which PHI is discussed should be made, to the extent possible, in a manner and location that protects the confidentiality of the information discussed.
    - Conversations with patients or a patient's family members in public areas should be conducted in a lowered voice, to the extent possible, so that unauthorized individuals cannot overhear the discussion. In emergency situations or where a patient is hearing impaired, take reasonable precautions to limit discussion of PHI.
    - Avoid using PHI in conversations in public areas, such as hallways or elevators.

3. Protecting Electronic PHI:
    - Store all PHI, Personally Identifiable Information ("PII"), and NYU Langone Health data on the network drive unless absolutely necessary to perform your job duties. If data must be stored on a portable device, that device must be encrypted (e.g., Iron Key).

- Emails containing PHI, PII, or other sensitive data to all non-NYU Langone Health domain recipients (i.e., non- @nyulangone.org or @med.nyu.edu) must be sent using NYU Langone Health's secure, encrypted email, SendSafe.
- If it is necessary to email PHI, only include the minimum amount of PHI necessary. Only send to the minimum number of recipients necessary, or those who 'need to know' to perform their jobs.
- All laptops and portable devices, used to store NYU Langone Health data, must be encrypted.
- Do not store any NYU Langone Health data, including PHI or employee information, on an unencrypted USB or external drive. The use of unencrypted USBs or external drives to store NYU Langone Health data will result in disciplinary action. If necessary to perform your job duties, encrypted Iron Key USB drives are available from Medical Center Information Technology ("MCIT") by submitting a ticket to the MCIT Service Catalog.
- PHI or PII may not be sent via text messaging (SMS), even if utilizing an MCIT managed device. SMS text messages are not secure. Other secure messaging systems may be available. Consult with the Privacy Officer and MCIT Security as necessary.

4. Protecting Written PHI:
    - All documents that contain PHI will be stored and maintained in a manner that minimizes the potential for incidental Use or Disclosure. Lock drawers and offices when possible.
    - Always double check, using double identifiers, to ensure that the correct paper document(s) is handed to the correct recipient.
    - All documents containing PHI will be properly disposed of, in compliance with all NYU Langone Health document retention and disposal policies.

5. NYU Langone Health will identify Workforce Members who need access to PHI to carry out their duties. When possible, restrictions to access only the minimum necessary amount of PHI to perform one's duties are used.

6. All Workforce Members are responsible for entries and queries under their unique user identity (e.g., Kerberos ID). Users must not share their IDs and password.

7. Workforce Members must log out of databases or electronic health record systems before stepping away or leaving a work station to prevent inappropriate access to patient information.

8. Access to areas that contain PHI are monitored and controlled to the extent reasonably possible (e.g., lock doors and file cabinets).

9. All Workforce Members will follow NYU Langone Health policies on proper destruction and disposal of PHI. Do not discard or reprovision any device containing PHI without first assuring the PHI has been removed or obliterated by MCIT. Consult MCIT for proper disposal of electronic devices.

10. Measures to ensure that PHI is adequately shielded to prevent unauthorized Disclosures will be used (e.g., privacy screens on computers in public areas).

Related Documents
All HIPAA Privacy Policies and Procedures
Medical Center Information Technology Security Policies
Medical Center Information Technology Workforce Members IT Policy
Privacy, Information Security, and Confidentiality Statement

Legal Reference
45 C.F.R. §164.530(c)

This version supersedes all NYU Langone Health (as defined in this Policy) previous policies, including but not limited to NYU Hospitals Center, New York University School of Medicine, Lutheran Medical Center, and Winthrop University Hospital.