DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information
PAGE: 1 of 4	**REPLACES POLICY DATED:** 11/1/11, 9/23/13
EFFECTIVE DATE: November 1, 2024	**REFERENCE NUMBER:** IP.PRI.013 (formerly HIM.PRI.013)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers and corporate departments, Groups, Divisions and Markets.

PURPOSE: To facilitate compliance with the Health Insurance Portability and Accountability Act (HIPAA) Standards for Privacy of Individually Identifiable Health Information (Privacy Standards), 45 CFR Parts 160 and 164, the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA), and any and all other Federal regulations and interpretive guidelines promulgated thereunder. To establish guidelines for mitigating inappropriate or unauthorized access, use and/or disclosure of Protected Health Information (PHI).

POLICY: In order to protect PHI when inappropriate or unauthorized access, use, and/or disclosure of PHI occur, the facility must take immediate, reasonable steps to mitigate the situation. The facility must review the administrative, physical, and technical safeguards in place to help ensure PHI is protected from further inappropriate and/or unauthorized access, use, and/or disclosure. This policy mainly addresses oral and paper-based PHI. Mitigation for issues involving electronic PHI (ePHI) and digital media is addressed in Information Protection and Security (IPS) policies, standards and procedures; and the Company's Responsible AI policy, EC.031; however, general mitigation requirements for ePHI and digital media are included for purposes of this policy.

States may have separate laws that may apply additional legal requirements. Consult your Operations Counsel to identify and comply with any such additional legal mandates.

Sanctions for issues involving improper safeguards will be applied in accordance with the facility's Sanctions for Privacy and Information Security Violations policy.

Refer to the HIPAA Privacy Standards, 45 CFR Parts 160.101 and 164.501, and IP.PRI.001, the Patient Privacy Program Requirements Policy, for definitions.

PROCEDURE:

For all situations involving the inappropriate or unauthorized access, use, and/or disclosure of PHI, thorough documentation of the facility's mitigation efforts must be created and maintained for a minimum of six (6) years. A HITECH risk assessment must be completed for all situations involving inappropriate or unauthorized access, use, and/or disclosure of PHI. In the event the situation meets the definition of a HITECH breach, notification to the patient, the Department of Health and Human Services, and if applicable, the media, will be made in accordance with the Protected Health Information Breach Notification policy, IP.PRI.011.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information
PAGE: 2 of 4	**REPLACES POLICY DATED:** 11/1/11, 9/23/13
EFFECTIVE DATE: November 1, 2024	**REFERENCE NUMBER:** IP.PRI.013 (formerly HIM.PRI.013)
APPROVED BY: Ethics and Compliance Policy Committee	

For situations involving workforce members removing PHI from the facility without authorization, the facility must make every attempt to facilitate the return of the documents. Facilities may work with labor and/or operations counsel to determine appropriate actions in those situations.

Faxing PHI

In the event the facility determines a fax has been inappropriately sent, the following mitigation efforts must be taken:

A. Contact the recipient and request that the fax be shredded or returned to the facility. If the recipient will shred the fax, obtain written confirmation of the destruction of the fax.

B. Correct fax directories or pre-programmed numbers that contain incorrect fax numbers.

Paper Documents Containing PHI

In the event documents containing PHI are accessed, used, and/or disclosed inappropriately or without authorization, the following mitigation efforts must be taken, as applicable:

A. If the incorrect PHI is given to a patient or the incorrect patient receives PHI, the facility must make attempts to retrieve the PHI or request that the PHI be destroyed. Documentation supporting the attempts to retrieve the PHI and supporting the mitigation attempts (*e.g.,* requesting that the PHI be destroyed) must be included as part of the facility's investigation documentation.

B. Efforts must be made to account for documents containing PHI left unattended or visible after hours and steps must be taken to ensure a process is in place to prevent any occurrence in the future.

C. The facility must make every effort to locate documents containing PHI that may be left, lost or stolen (*e.g.,* left in a taxi). Examples of efforts include, but are not limited to, making calls to the company, checking lost and found desks, reviewing security tapes when appropriate, and filing police reports.

Oral Communications Involving PHI

Mitigation efforts for situations involving inappropriate or unauthorized oral communications include, but are not limited to:

A. Requesting that the offending parties lower their voices or terminate the conversation.

B. Evaluating existing policies and/or procedures to determine if revisions should be made.

C. Providing awareness and education via posters, newsletters, and other general reminders of safeguarding requirements.

D. In situations involving inappropriate observers present, workforce members must inform the observer that he/she is not permitted to observe and/or must notify the workforce member's supervisor immediately.

General Mitigation for Situations Involving Electronic Devices

In situations where an electronic device was inappropriately or without authorization accessed, used, displayed or disclosed, facilities must follow all Information Protection policies and standards, in particular standards Incident Reporting and Response Procedures, IM.MISI.01. However, general mitigation efforts include, but are not limited to:

A. For situations involving PHI viewed on an inappropriately placed computer monitor, a review of the facility's monitor placements and use of screen savers must be made.

B. In the event a device containing PHI is lost or stolen, the facility must:

1. Conduct a thorough and immediate investigation and search to facilitate finding and retrieving the device:

    i. Work with operations and labor counsel, if applicable.

    ii. Interview workforce members and/or former workforce members, if applicable, and obtain written attestations that information will not be further used or disclosed.

    iii. If the device is believed to be stolen:

        1. Review security tapes, if available.

        2. File a police report.

2. Work with IPS and ITG to verify whether the device was appropriately encrypted and to recreate the information believed to be contained on the device. In the event the device was not encrypted or the facility's policies and procedures for the use of personal devices was not followed, a thorough review of the facility's devices, policies and procedures must be conducted to ensure there is not additional risk of further inappropriate access, use and/or disclosure of PHI.

General Mitigation for Situations Involving Digital Media

A. In situations where PHI was inappropriately or without authorization accessed, used, displayed or disclosed through Digital Media, facilities must follow all Information Protection policies and standards including Incident Reporting and Response IM.MISI.01.

B. In the event of a situation where PHI was inappropriately or without authorization accessed, used, displayed, or disclosed through Digital Media, general mitigation efforts include, but are not limited to:

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information
PAGE: 4 of 4	**REPLACES POLICY DATED:** 11/1/11, 9/23/13
EFFECTIVE DATE: November 1, 2024	**REFERENCE NUMBER:** IP.PRI.013 (formerly HIM.PRI.013)
APPROVED BY: Ethics and Compliance Policy Committee	

1. Review of the Digital Media through which the PHI was inappropriately or without authorization accessed, used, displayed or disclosed.
2. Conduct a thorough and immediate investigation and search to facilitate identifying how the PHI was inappropriately or without authorization accessed, used, displayed or disclosed through the Digital Media:
    i. Work with IPS, ITG, and labor counsel, if applicable.
    ii. Interview colleagues and/or former colleagues, if applicable, and obtain written attestations that information will not be further used or disclosed.
3. In the event the Company's policies and procedures for the use of Digital Media were not followed, a thorough review of the Colleague's devices, Digital Media, and actions must be conducted to ensure there is not additional risk of further inappropriate access, use and/or disclosure of PHI.

DEFINITIONS:

Digital Media refers to any and all digital technology, platform and/or practice (both now existing or existing in the future) that enables people to use, create, share, or otherwise interact or engage with content, individuals, communities, opinions, insights, and/or conversations over the internet.

REFERENCES:

1. Patient Privacy Program Policies, IP.PRI.001 – IP.PRI.013
2. Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information 45 CFR Part 164
3. American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D
4. Information Protection Policies, IP.SEC.001 – IP.SEC.021
5. Information Protection Standard: Incident Reporting and Response Procedures, IM.MISI.01
6. Records Management Policy, EC.014
7. Responsible AI Policy, EC.031
8. HCA Healthcare Digital Media Guidelines