DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Safeguarding Protected Health Information
PAGE: 1 of 5	**REPLACES POLICY DATED:** 11/1/11
EFFECTIVE DATE: September 23, 2013	**REFERENCE NUMBER:** IP.PRI.012 (formerly HIMI.PRI.012)
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 protecting and safeguarding protected health information (PHI).

POLICY: The facility must take reasonable steps to safeguard and protect PHI. The facility must identify and utilize appropriate administrative, physical, and technical safeguards in order to protect PHI from inappropriate and/or unauthorized access, use, and/or disclosures. In particular, the facility must take additional steps to protect patient, patient personal representative, and guarantor social security numbers (SSNs) (*e.g.,* masking or removing the SSNs from documents and/or systems) to help guard against identity theft and financial harm to patients and others. This policy addresses oral and paper-based PHI. Safeguarding requirements for electronic PHI (ePHI) (*e.g.*, encryption) are addressed in Information Protection policies, standards and procedures; however, general requirements 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:

<u>Faxing PHI</u>

When faxing PHI, workforce members should take appropriate safeguards:

1. Locate fax machines in low-traffic areas and inaccessible to visitors.
2. Consider whether it is appropriate to fax the PHI (*e.g.,* is there another secure method to send the information, is the recipient authorized to receive the information, is the PHI particularly "sensitive").
3. Confirm telephone requestors by returning the phone call prior to sending.
4. Verify the fax number before sending.
5. Use a fax coversheet.

6. Double check the fax number entered before sending.
7. Set the fax machine to print an auto-confirmation page, if available, and check the confirmation page to ensure:
    i. Delivery was successful, and
    ii. Correct fax number was dialed
8. Use pre-programmed fax numbers, if available
    i. Test pre-programmed fax numbers prior to use.
    ii. Have a process in place to verify the programmed numbers on a regular basis.
    iii. Remind regular fax recipients to provide updated fax numbers when numbers change.

<u>Paper Documents Containing PHI</u>

Facilities must ensure that reasonable safeguards are in place to protect paper documents containing PHI:

1. To the extent feasible:
    i. PHI should be removed from high visibility areas, even if those areas are not open to the public, and
    ii. PHI should be maintained in a confidential manner in order to prevent workforce members and others that do not have a need to know from accessing such PHI.
    iii. Documents must not be left unattended in areas accessible to the public (*e.g.*, charts may not be left unattended on a counter that is open to the public).
    iv. Access to areas containing PHI must be limited to authorized personnel.
2. Documents containing PHI must be disposed of securely (*e.g.,* place PHI in shred bins not regular trash cans or recycle bins that will not be shredded). The facility must eliminate unnecessary regular trash cans.
3. Mail and package delivery (*e.g.*, US Postal Service, Fed Ex) pick-up sites should be in a separate location from employee desks or customer counters to help avoid the wrong information being picked up.
4. Facilities must have a process in place to verify documents are for the correct patient prior to providing the documents to the recipient (*e.g.,* verify recipient and content prior to giving discharge papers to an individual).
5. Facilities may not send mailings to individuals if the clinic or facility name on the postcard or envelope seems likely to reveal a patient's sensitive diagnosis (*e.g.,* Medical Center HIV clinic, City Oncology Center).
6. Any removal of documents containing PHI from any office or facility must be with the workforce member's manager's advance approval. Only the minimum necessary amount of information required to perform the job function may be approved. The workforce member is responsible for ensuring the documents are safeguarded at all times and promptly returned to the office or facility. Safeguarding examples include, but are not limited to:
    i. Logging the PHI that will leave the office or facility. PHI should not leave any office or facility unless another copy of the PHI removed remains at the office or facility.

ii. Ensuring PHI is not left in an unsecured area (*e.g.,* an unlocked vehicle or a locked vehicle in which the PHI is in plain view or is held in a visible container that may encourage theft such as a box of records, a briefcase, or a laptop computer case.)

Oral Communications Involving PHI

Workforce members may only discuss PHI with other authorized workforce members who have a legitimate "need to know" or with others as permitted by the HIPAA Privacy Rule. Facilities must ensure that reasonable safeguards are in place when workforce members verbally communicate PHI including:

1. Workforce members must follow the facility's "Verification of Requestors" policy for telephone communications involving PHI.
2. When leaving messages on answering machines, workforce members must use professional judgment to ensure that such disclosures are in the best interest of the individual and that only the minimum necessary PHI is disclosed.
    i. If the information is necessary to ensure quality care, any and all information may be left, including PHI. The information may include:
        a. Pre-operative instructions (*e.g.*, don't eat nor drink after midnight, take "x" medications).
        b. Urgent follow-up care is required. A voicemail message may be left for the patient stating:
            a. The provider name,
            b. Who the caller is trying to reach,
            c. It is urgent that the patient call to discuss his/her recent treatment,
            d. The return telephone number of the provider, and
            e. With whom the individual should ask to speak with when returning the call.
    ii. To confirm appointments, workforce members must ensure that the facility, practice, center, or physician's name would not potentially reveal a sensitive diagnosis (*e.g.,* Medical Center HIV clinic, City Oncology Center).
3. Facilities are permitted to use patient sign-in sheets or call out patient names in waiting rooms provided that the information disclosed is appropriately limited per minimum necessary standards and reasonable safeguards are in place (*e.g.,* sign-in sheets do not require the patient to indicate the reason for being seen, removable labels are utilized).
4. Workforce members must take reasonable safeguards and precautions when discussing PHI. The HIPAA Privacy Rule exempts certain oral treatment communications in order to ensure a provider's primary concern is the treatment of the patient. In emergency situations, providers may engage in communications as required for quick, effective, and high quality health care. When appropriate and practicable, suggested safeguard examples include, but are not limited to:
    i. Using lowered voices;
    ii. Closing the curtain in semi-private rooms;

iii. Speaking apart from others;
iv. Refraining from discussing PHI in elevators, cafeterias, or other public areas; and
v. Asking visitors to leave the room or obtaining patient consent prior to speaking in front of visitors.

5. Workforce members are not permitted to bring friends or family members to work, to observe, or help with work related tasks if the friends or family members will have access to patients or patient information.

General Safeguards for Electronic Media

A. Workforce members must take appropriate safeguards to limit disclosure of PHI at workstations and other areas where computer monitors may be located:
   1. Computer monitors must be positioned away from the direct view of the general public.
   2. Password protected screensavers must be in place on computer monitors.
   3. Passwords must not be displayed or viewable (*e.g.,* attached to the monitor).
   4. Refer to Corporate Information Protection Physical Security Standards for more details.
B. The Information Protection Department maintains Policies, Standards, guidance, and procedures which outline comprehensive administrative, physical and technical safeguards to PHI which is stored on electronic media (ePHI), including detailed encryption requirements. For the purposes of this policy, facilities must ensure that:
   1. No media (*e.g.*, cellular telephones, flash or "thumb" drives, laptop computers, workstations) are used to access or store PHI without appropriate encryption and authorization. Refer to Corporate Information Protection Standards for more details.
   2. No personal media may be used to connect to the Company network, or to access or store PHI (or any type of Company data), unless specifically approved using the procedures outlined in Information Protection Guidance: Connecting Non-Company PCs. This guidance defines the approval process and the specific data safeguards that must be in place (including, but not limited to, encryption).
   3. Only mobile devices with sufficient security controls, including encryption capabilities, may connect to the Company network. Required approvals vary, and are listed on the Mobile Device Request Form. Completed Forms with signed approvals must be sent to the Corporate IT&S Asset Management team for final review and approval. See references below for more information about which devices are allowed to connect, the types of data access permitted, and the approval process. Also refer to the Information Protection site on Atlas, and the Asset Management Mobile Device Portal on Atlas.

All Company employees, workforce members, and any other individuals who have potential access to Company sensitive data (including PHI), must sign the Company Confidentiality and Security Agreement (CSA) pursuant to the Information Confidentiality and Security Agreements Policy, IP.SEC.005.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Safeguarding Protected Health Information
PAGE: 5 of 5	**REPLACES POLICY DATED:** 11/1/11
EFFECTIVE DATE: September 23, 2013	**REFERENCE NUMBER:** IP.PRI.012 (formerly HIMI.PRI.012)
APPROVED BY: Ethics and Compliance Policy Committee	

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 Standards
6. IT&S Asset Management Mobile Device Portal
7. Information Protection Guidance: Workstation Security
8. Sending Sensitive Data
9. Reporting Lost or Stolen Devices
10. IP Guidance Connecting Non-Company PCs and Devices