DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Protecting and Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Personally- Identifiable Information (PII)
PAGE: 1 of 5	**REPLACES POLICY DATED:** 9/1/14, 5/1/15
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.GEN.002
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: All facilities are responsible for the protection of personally-identifiable information (PII). This policy illustrates the areas in which appropriate actions must be taken to ensure the use of PII is limited and protected. For purposes of this policy, if information may be considered both PII and PHI, IP.PRI.012 must be followed. Refer to IP.PRI.001 for the definition of PHI, IP.PRI.012, Safeguarding Protected Health Information (PHI), for the protection of PHI, and IP.PRI.013, Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of PHI.

POLICY: When PII is maintained it is at risk in both its electronic and physical forms. PII must be protected with administrative, technical, and/or physical safeguards, as appropriate, while it is processed, accessed, stored, or otherwise used. Facilities must have adequate processes and procedures in place to protect the PII against unauthorized disclosure, access, or misuse. In particular, the facility must take additional steps to protect 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.

In order to protect PII when inappropriate or unauthorized access, use, and/or disclosure of PII 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 PII is protected from further inappropriate and/or unauthorized access, use, and/or disclosure.

This policy addresses oral, paper-based and electronic PII. Additional safeguarding and mitigation requirements for electronic PII (*e.g.*, encryption) are addressed in Information Security standards and procedures; however, general requirements are included for purposes of this policy.

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

DEFINITION

Personally-Identifiable Information (PII) – Any information that can be used alone or with other sources of information to uniquely identify, contact, or locate an individual. The following list contains examples of information that may be considered PII:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Protecting and Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Personally- Identifiable Information (PII)
PAGE: 2 of 5	**REPLACES POLICY DATED:** 9/1/14, 5/1/15
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.GEN.002
APPROVED BY: Ethics and Compliance Policy Committee	

financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other; distinguishing characteristic), fingerprints, or other biometric image or template data (*e.g.,* retina scan, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration number, title number, license plate number and related information; and
- Information about an individual that is linked or linkable to one of the above (*e.g.,* date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

PROCEDURE:

1. Facilities must ensure that the minimum amount of PII is collected to conduct business, the access to and use of PII is limited to those individuals who need the information to perform job duties and proper controls are in place, where feasible, to protect the data quality and integrity of PII. Practices for the collection of PII:
   - Obtain PII by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
   - Wherever possible, controls must be in place to ensure that PII is accurate, relevant, timely, and complete for the purposes for which it is to be used.
   - Reasonable steps must be made to confirm the accuracy and relevance of PII.
   - Procedures must be in place to maintain collected PII and ensure the information that is maintained is up-to-date.

2. Facilities must consider the nature in which PII is used and develop appropriate administrative, technical and/or physical safeguards surrounding each process that exposes PII to risks such as loss or unauthorized access, destruction, modification or disclosure of data. . These safeguards must reflect:
   - The sensitivity of the data being processed, stored and accessed;
   - The environment in which the data is processed, stored and accessed;
   - The risk of exposure; and
   - The cost of the safeguard under consideration.

3. To the extent feasible, when designing information systems, facilities must employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII.

4. When appropriate, facilities must minimize access to and transmission of PII data fields in any form (*e.g.,* electronic, paper, verbal). Mask, redact and/or use other anonymization and de-identification techniques to reduce the sensitivity of PII and decrease the risk resulting from its use.

5. The facility must retain and dispose of PII as determined in the Company's Records Management Policy, EC.014. Electronic materials containing PII must be sanitized or handled, if applicable, as stated in Information Security Standards AM.MH.01, AM.MH.02, and AM.MH.03.

6. Workforce members must take reasonable and appropriate actions to ensure the protection of PII and to maintain the privacy of individuals.

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

Mitigation:

For all situations involving the inappropriate or unauthorized access, use, and/or disclosure of PII, mitigation efforts must be taken and thorough documentation of those efforts must be created and maintained in accordance with Records Management Policy, EC.014. Mitigation efforts include, but are not limited to:

<u>Faxing Documents Containing PII</u>

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 or email confirmation of the destruction of the fax.
B. Correct fax directories or pre-programmed numbers that contain incorrect fax numbers.

<u>Paper Documents Containing PII</u>

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

A. If the incorrect PII is given to a recipient or an unauthorized recipient receives PII, the facility must make attempts to retrieve the PII or request that the PII be destroyed. Documentation supporting the attempts to retrieve the PII and supporting the mitigation attempts (*e.g.,* requesting that the PII be destroyed) must be included as part of the facility's investigation documentation.
B. Efforts must be made to account for documents containing PII 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 PII 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 PII

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, employees must inform the observer that he/she is not permitted to observe and/or must notify the employee'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 standard Incident Reporting and Response IM.MISI.01. However, general mitigation efforts include, but are not limited to:

A. For situations involving PII 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 PII 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 employee and/or former employees, 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 the Information Protection Program and IT&S 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 PII.

State Breach Notification Requirements:

Facilities must comply with their state breach notification laws and must follow any policies and procedures addressing the State-specific requirements. Facilities must work with their assigned operations counsel to identify and comply with any such additional legal mandates or contact the Information Protection mailbox.

REFERENCES:

1. Patient Privacy Program Requirements Policy, IP.PRI.001
2. Safeguarding Protected Health Information Policy, IP.PRI.012
3. Mitigating Inappropriate or Unauthorized Access, Use and/or Disclosure of Protected Health Information Policy, IP.PRI.013
4. NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
5. NIST SP 800-53 rev. 4 - Appendix J – Privacy Control Catalog
6. Records Management Policy, EC.014
7. Information Protection - Release of Company Data to External Entities, IP.GEN.004
8. Information Confidentiality and Security Agreements Policy, IP.SEC.005
9. IS Standard: Media Handling AM.MH.01, AM.MH.02 and AM.MH.03
10. IS Standard: Incident Reporting and Response, IM.MISI.01