DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Protected Health Information Breach Risk Assessment and Notification
PAGE: 1 of 4	**REPLACES POLICY DATED:** 9/23/09, 10/12/09, 9/23/13
EFFECTIVE DATE: May 1, 2017	**REFERENCE NUMBER:** IP.PRI.011 (formerly HIM.PRI.011)
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 Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) breach notification of unsecured protected health information (PHI) requirements and any and all other Federal regulations and interpretive guidelines promulgated thereunder.

POLICY: Any Company-affiliated facility in the case of a breach of unsecured PHI, must notify the patient or their personal representative without unreasonable delay and in no case later than 60 days of discovering the breach.

A breach is considered discovered as of the first day on which the breach is known by the business associate and/or facility. Business associates are required to report any breach to facilities immediately after discovery.

If a law enforcement official determines that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under §164.528(a)(2) of title 45, Code of Federal Regulations.

All Company-affiliated facilities, primarily led by the Facility Privacy Official (FPO), must work to timely and accurately report any breach of unsecured PHI according to company policy, ARRA, and any and all other Federal and State regulations and interpretive guidelines promulgated there under. The FPO must maintain all documentation related to the breach (*e.g.*, notification letters) for a minimum of six (6) years.

Facilities in States with additional or more restrictive breach notification laws must develop and implement policies and procedures addressing the State-specific requirements.

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.

A breach is any impermissible acquisition, access, use, or disclosure of unsecured protected health information which compromises the security or privacy of such information. To determine if a breach has occurred, a risk assessment must be performed to determine the probability that the security or privacy of the PHI has been compromised. The requirements outlined in the HITECH Breach Risk Assessment and Notification Process must be followed. Limited Data Sets are subject to the breach notification reporting requirements. The term ‘breach’ does not include:

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Protected Health Information Breach Risk Assessment and Notification
PAGE: 2 of 4	**REPLACES POLICY DATED:** 9/23/09, 10/12/09, 9/23/13
EFFECTIVE DATE: May 1, 2017	**REFERENCE NUMBER:** IP.PRI.011 (formerly HIM.PRI.011)
APPROVED BY: Ethics and Compliance Policy Committee	

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if
    - Such acquisition, access, or use was made in good faith and within the course and scope of authority;
    - Such information is not further used or disclosed in a manner not permitted; or
2. Any inadvertent disclosure by a person who is authorized to access PHI at the same covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates; and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
3. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Except for the exclusions listed in 1-3 above, an impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach unless the covered entity, or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

PROCEDURE: Any Company-affiliated facility in the case of a potential breach of unsecured PHI must follow the HITECH Breach Risk Assessment and Notification Process to ensure a risk assessment is performed to determine the probability that the security or privacy of the PHI has been compromised. If the risk assessment indicates a breach has occurred, the Company-affiliated facility must notify the patient or their personal representative without unreasonable delay and in no case later than 60 days of discovering the breach.

Notification:

Patient Notification

1. After a complete investigation, no later than 60 days from breach discovery, the facility must provide written notice to the patient or:
    a. If the patient is deceased, the next of kin or personal representative.
    b. If the patient is incapacitated/incompetent, the personal representative.
    c. If the patient is a minor, the parent or guardian.

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Protected Health Information Breach Risk Assessment and Notification
PAGE: 3 of 4	**REPLACES POLICY DATED:** 9/23/09, 10/12/09, 9/23/13
EFFECTIVE DATE: May 1, 2017	**REFERENCE NUMBER:** IP.PRI.011 (formerly HIM.PRI.011)
APPROVED BY: Ethics and Compliance Policy Committee	

2. Written notification must be in plain language at an appropriate reading level with clear syntax and language with no extraneous materials. Americans with Disabilities Act (ADA) and Limited English Proficiency (LEP) requirements must be met.
   Written notification must be sent to the last known address of the patient or next of kin via first class mail, or if specified by the patient, by encrypted electronic mail. Certified mail must not be used. The Company's template letter must be used when sending written notification to a patient, personal representative, or next of kin.
3. In the case where there is insufficient or out-of-date contact information:
   a. For less than ten (10) individuals that precludes direct written notification to the patient, a substitute form of notice shall be provided such as a telephone call.
   b. In the case that there are ten (10) or more individuals for which there is insufficient or out of date contact information and contact information is not obtained, the facility must:
      i. Post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or
      ii. Provide notice in major print or broadcast media in the geographic area where a patient can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number must be included in the notice. If the facility utilizes major print or broadcast media, the FPO must work with the corporate Information Protection Department to coordinate this notification.
4. If the facility determines the patient should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, the facility may, in addition to providing notice as outlined in steps 2-4 above, contact the patient by telephone or other means, as appropriate.

Media Notification

1. In the case where a single breach event affected more than 500 residents of the same State or jurisdiction from a single facility, notice shall be provided to prominent media outlets. A jurisdiction is defined as a geographic area smaller than a state (*e.g.*, city, county). For example, if a single breach event affects 200 patients in Florida and 400 patients in Texas, a notice to the media is not required because there were not more than 500 patients in the same State or jurisdiction affected. However, if a single breach event affects 500 patients in Florida and 500 in Texas, a media notice is required in both Florida and Texas.
2. The written notification must contain the same elements as the patient notification.
3. The FPO must work with the corporate Information Protection Department to coordinate this notification.

HHS Notification

1. Notice must be provided by the facility contemporaneously with patient notification, without unreasonable delay and in no case later than 60 days from the breach discovery to the Secretary of the Department of Health and Human Services (HHS) if a single breach event

DEPARTMENT: Information Protection	**POLICY DESCRIPTION:** Protected Health Information Breach Risk Assessment and Notification
PAGE: 4 of 4	**REPLACES POLICY DATED:** 9/23/09, 10/12/09, 9/23/13
EFFECTIVE DATE: May 1, 2017	**REFERENCE NUMBER:** IP.PRI.011 (formerly HIM.PRI.011)
APPROVED BY: Ethics and Compliance Policy Committee	

was with respect to 500 or more individuals regardless of the State or jurisdiction. Facilities must use the electronic form available on the HHS website when notifying HHS of breaches involving 500 or more individuals.

2. If a breach is with respect to less than 500 individuals, the facility must use the electronic form available on the HHS website and submit to HHS no later than 60 days after the end of the calendar year in which the breach was discovered.
3. Facilities must maintain a log of any breaches meeting the HITECH definition that occur during a calendar year.

Content of Notification:

Regardless of the method by which the notice is provided to patients, notice of the breach must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured PHI that were involved in the breach, such as full name, Social Security Number, date of birth, home address, account number, diagnosis code or disability code. Only the generic type of PHI should be listed in the notice (*i.e.*, date of birth rather than the patient's actual birth date).
3. To the extent possible, the steps the individual should take to protect him/her from potential harm resulting from the breach (*e.g.,* credit monitoring when financial information or social security number is disclosed).
4. A brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individual, and to protect against any further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

REFERENCES:

1. American Recovery and Reinvestment Act of 2009
2. Health Insurance Portability and Accountability Act (HIPAA), Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164
3. Privacy Program Policy, IP.PRI.001
4. HITECH Breach Risk Assessment Template
5. HITECH Breach Patient Notification Letter Template
6. HITECH Breach Risk Assessment and Notification Process
7. Facility Model Policy, Sanctions for Privacy and Information Security Violations