Effective Date: 01/14/2009 010-Breach Notification Policy
Review Dates: 6/29/13,
Revision Date: 11/14/2011

CATHOLIC HEALTH SERVICES
Rockville Centre, New York
IT Security & Privacy Policies and Procedures
Policy Number: 010

Effective Date:
12/16/2005

Last Revision Date:
11/14/2011

TITLE: 010-Breach Notification Policy

PURPOSE:
Catholic Health Services of Long Island ("CHS") and its contractors and vendors will strive to prevent breaches of Unsecured Protected Health Information ("PHI") and personal information ("PI") electronically or otherwise, and maintain privacy and security measures to protect the confidentiality of PHI and PI. This policy describes the process by which CHS will assess a potential breach and appropriately notify individuals regarding a confirmed breach of security when Unsecured PHI has been acquired, assessed, used by or disclosed to an unauthorized person. Pursuant to the Health Insurance Portability and Accountability Act ("HIPAA") and Regulations promulgated there under, CHS will notify individuals when Unsecured PHI has been acquired, accessed, used or disclosed by an unauthorized person, when a confirmed breach of the security of the system does not fall within a statutory exception or there is not a low probability that the PHI has been compromised.

POLICY:

1. The CISO and/or the Privacy Officer, who in addition to undertaking the appropriate steps set forth in the Security Incident Response Policy, will promptly notify the following individuals of the unauthorized access, use or disclosure:

a. CHS Chief Information Security Officer

b. CHS Privacy Officer

c. CHS Chief Information Officer ("CIO")

d. CHS Chief Medical Officer

e. CHS Deputy General Counsel

f. CHS Senior Vice President of Risk Management

g. Public Affairs, following consultation with counsel.

2. Confirmed breaches of the security or privacy of Unsecured PHI will invoke certain actions to determine the probability that the PHI has been compromised based on a risk assessment and, under specific circumstances, notification of the breach will be made to the affected individual(s). When a confirmed breach has been determined, the breach response team will be assembled and an investigation into the breach will be conducted. The response team will be comprised of those persons listed above, as appropriate.

3. PI is identified as unencrypted computerized or written information that is not rendered unreadable and indecipherable that can identify an individual, combined with one or more of the following data elements:

a. Social Security number;

b. Medical insurance number, including Medicare/Medicaid;

c. Driver's license number or non-driver identification card;

d. Account number, or credit/debit card number in combination with security access codes or PIN numbers that would permit access to an individual's financial accounts; or

e. Sensitive health information;

f. Other personal data elements such as address and date of birth.

4. For purposes of this Policy, computerized PI is considered to be unencrypted when either the identifying information or the data element is not encrypted or is encrypted with a key that has also been acquired without authorization.

5. If encrypted computerized PI is compromised, along with the corresponding encryption key, the information will be considered unencrypted.

6. PI does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.

7. Procedure:

a. CHS has implemented reasonable and appropriate Administrative, Physical and Technical Safeguards to protect the confidentiality, integrity and availability of PHI and PI in its possession.

b. CHS has implemented reasonable systems for the discovery and reporting of a breach of PHI or PI. A "breach" of PHI is the unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI.

c. When a breach has been reported, an investigation into the breach will be conducted.

d. The investigation and steps taken will be thoroughly documented. If the conclusion of the investigation is that no breach occurred, no further action is necessary, but the investigation and conclusion will be thoroughly documented.

e. If it is confirmed that a breach of security or confidentiality has occurred and has resulted in the unauthorized disclosure of PHI, the following risk assessment steps will be taken:

i. Determine whether or not the information breached was Unsecured. Unsecured PHI includes information not secured through encryption or destruction, and is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary of HHS in guidance issued under Section 13402(h)(c) of Public Law 111-5.

ii. Determine the reasonable likelihood that such information was accessed by an unauthorized person.

iii. Determine the probability that the PHI has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (ii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated.

f. The risk assessment will be documented thoroughly, including the actions taken, the conclusions of the assessment and the basis for the determination that there was or was not a low probability that the PHI was compromised.

g. If it is determined that the information breached was secured and there is no reasonable likelihood that the secured information was rendered usable, readable or viewable by an unauthorized person, no further action is necessary, but the determination and conclusion will be documented.

h. If it is determined that the information breached was Unsecured, but the circumstance of the breach falls within one of the exceptions to HIPAA (45 C.F.R. § 164.42), so notification is not required, such determination will be documented.

i. If it is determined that the breach of the security of the system demonstrates that there is more than a low probability that the PHI was compromised, CHS will as soon as possible, but no later than 60 days after the discovery of the breach, notify the individual(s) whose information was disclosed as a result of the breach, and the determination and conclusion will be documented.

j. If it is determined that the information breached was Unsecured and notification is required, an analysis of the requirements for notification of the State in which the individuals reside will be conducted and documented.

k. If notification to law enforcement or another regulatory body or agency is required under State law, such notification will be made to the regulatory body or agency in accordance with State law.

l. If State law requires notification to the individual, notification will be made in accordance with State law.

m. Notification to the individual may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and the notification will be made after law enforcement determines it will not compromise its investigation.

n. Individuals affected by the breach will be directly notified by one of the following methods:

i. Written notice;

ii. Electronic notice (by e-mail), providing the person has agreed, in writing, to re receive such notice in electronic form and an log of each such notification is maintained by the CISO or the Privacy Officer;

iii. Telephone notification, provided that a log of each such situation is maintained by the CISO; or

iv. If applicable, if CHS demonstrates to the NYS Attorney General that the cost of providing notice would exceed $250,000; the affected class of subject persons to be notified exceeds 5,000; or CHS does not have sufficient contact information, notice may consist of the following:

1. E-mail, if e-mail address is known to CHS, without the prior written consent of the individual;

2. Conspicuous posting of the notice to the CHS Website; and

3. Notification to major statewide media.

o. Notification of a breach to affected individuals will be in plain language and include at a minimum:

i. a brief description of what happened, including the date of the breach and discovery of the breach;

ii. a description of the type of Unsecured PHI or other personal information that was involved in the breach;

iii. any steps individuals should take to protect themselves from potential harm resulting from the breach;

iv. a description of the investigation into the breach, mitigation of harm to individuals, and protection against further breaches; and

v. contact procedures, which will include a toll-free telephone number, an e-mail address, website or postal address.

p. The notification must include any additional information required by applicable State law.

q. If the breach involves more than 500 residents of a state or jurisdiction, notice will be provided to the media and to the Secretary of the Department of Health and Human Services ("HHS") contemporaneously.

r. A log of any and all breaches of Unsecured PHI of less than 500 individuals will be maintained and reported to the Secretary of HHS on an annual basis.

s. Business Associates and vendors, through their contracts and/or Business Associates Agreements with CHS will be required to provide notification of a breach to CHS so affected individuals can be notified, as necessary. Business Associates must provide all available information without delay.

t. Documentation will be maintained of each individual notified, each notification provided to HHS and any other notification to the Secretary of HHS as required by law, by the CISO.

u. If legally required, the CISO or the Privacy Officer will notify the New York State Office of Cyber Security and Critical Infrastructure Coordination, the NYS Attorney General, and the NYS Consumer Protection Board as to the timing, distribution, content, and number of persons affected on the standard form.

v. When more than 5,000 individuals are to be notified at one time, the CISO or the Privacy Officer will notify a consumer reporting agency as to the timing, content and distribution of the notices and the approximate number of affected individuals.

ENFORCEMENT

1. The CHS CISO has general responsibility for implementation of this policy, as well as the standards defined or implied by this policy. Members of our CHS staff and Medical Staff who violate this policy will be subject to disciplinary action in accordance with the Information Security Disciplinary Policy, up to and including termination of employment or contract with CHS. Vendors who are found to be in violation of this policy will be considered to be in breach of contract which may result in disciplinary action up to and including termination of contract, and possible legal actions.

2. Anyone who knows or has reason to believe that another person or entity has violated this policy should report the matter promptly in accordance with applicable policy and procedure. All reported matters will be investigated, and, where appropriate, steps will be taken to remedy the situation. Where possible, CHS will make every effort to handle the reported matter confidentially. Any attempt to retaliate against a person for reporting a violation of this policy will itself be considered a violation of this policy that may result in disciplinary action up to and including termination of employment. Vendors who are found to be in violation of this may result in disciplinary action up to and including termination of contract, and possible legal actions.

EXCEPTIONS

Exceptions to this policy can be made with written approval of both the CISO and CHS Chief Information Officer (CIO).

REVIEW OF POLICY

In the event that a significant regulatory change occurs, the policy will be reviewed and updated as needed. The policy will be reviewed periodically to determine its effectiveness in complying with the HIPAA Security Regulations, as well as meeting business needs.

Approved By:
Marcy Dunn, CIO Date
Patrick Darienzo, CISO Date
Lynn Taylor, CPO Date
Dr. Patrick O'Shaughnessy, CMO Date