General Information

Policy Name:	HIPAA: Notification Process for Unsecured PHI Breach
Category:	Risk Management – Corporate Compliance
Applies To:	All Staff
Key Words:	Breach, HIPAA, Notification, Risk, Assessment, Breach, Log, Disclosure
Associated Forms & Policies:	
Original Effective Date:	01/01/10
Review Dates:	02/01/12, 08/01/13, 07/03/17, 08/30/21, 11/07/22, 11/06/23
Revision Dates:	03/03/15, 08/22/18, 09/27/19
This Version's Effective Date:	09/27/19

Policy

It is the policy of Crouse Hospital to ensure that proper due diligence is performed and notification is provided to our customers (patients, physicians, employees) when a breach of protected health information (PHI) occurs. Crouse Hospital takes the safeguarding of patient information very seriously and will follow guidelines set forth by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and modifications contained in the HIPAA Omnibus Rule of 2013. Crouse will implement and maintain procedures used to respond to a breach incident as well as provide breach notifications as required under HIPAA, HITECH and any other federal and state laws.

Procedure

Investigation & Risk Assessment:

Following the discovery of a potential breach incident, Crouse will begin an investigation to determine whether or not the Privacy Rule has been violated. Any potential violations are considered a breach unless a risk assessment demonstrates that there is a low probability that the privacy and security of PHI has been compromised. The risk assessment must address four critical factors:

- The type of PHI and/or number or type of identifiers and the likelihood of re-identification
- The unauthorized individual(s) to whom the PHI was impermissibly disclosed to or used
- Determination of whether or not the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated

Breach investigations, including any notifications, will be conducted by the Privacy and Security Officers, with assistance from the Corporate Compliance and Risk Management departments. The investigators will seek assistance from other departments such as Human Resources, Information Technology, and others where necessary.

Risk Assessment

Once a potential breach has been discovered by a representative of Crouse Hospital or a Business Associate, a

risk assessment must be conducted to determine whether or not an impermissible use or disclosure of PHI occurred. A four-factor risk assessment must be conducted to establish the probability that PHI has been compromised; the following are the four factors that must be considered in the risk assessment:

1. The nature and extent of the PHI involved.
    a. What type of patient identifiers were involved in the disclosure?
    b. Based on the type of PHI disclosed, what is the probability that an individual could be re-identified?
    c. Considering the type of PHI involved, could it be used by the unauthorized recipient to benefit their own interests?
2. The unauthorized individual who used or received the PHI.
    a. Consider the unauthorized person who impermissibly used the protected health information or to whom the impermissible disclosure was made.
    b. Does the unauthorized recipient have their own obligations to protect PHI?
3. PHI was actually acquired or viewed.
    a. Is there evidence that PHI was accessed or viewed, or was there only an opportunity for PHI to be accessed or viewed?
4. Determine the extent of which the risk to PHI has been mitigated.
    a. Have satisfactory assurances that the information will not be used, disclosed, or destroyed been obtained through a confidentiality agreement or other means?
    b. Determine the extent and effectiveness of the risk mitigation.

If the above steps fail to demonstrate that there is a low probability that PHI has been compromised, breach notification is required.

If it has been determined that a breach has occurred the following notifications must occur:

1. Individual Notification
    a. Crouse and any Business Associate involved will notify the individual(s) affected without unreasonable delay and no later than 60 days from the date of discovery. Notification will be made by the Privacy Officer via first class mail (or any method specified by the individual's preference) at the last known address. Any reasons for delay in notification will need to be documented and evidence will be shown which demonstrates the hold up.
    b. If the breach involves 10 or more individuals whose contact information is out of date, a notice will be posted on Crouse's website for at least 90 days (www.crouse.org) or in a major print or broadcast media outlet where the individuals likely reside. The Privacy Officer will involve the Communications department as well as Senior Leadership.

2. Notification to Health and Human Services (HHS) Secretary & NYS Attorney General
    a. In addition to notifying the affected individual(s), Crouse must notify the Health and Human Services (HHS) Secretary by visiting the HHS website and electronically submitting the breach report form. (https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html)
        i. For a breach involving less than 500 individuals, notification will be made without unreasonable delay and no later than the end of the calendar year in which the breach was discovered.
        ii. For a breach involving 500 or more individuals, notification will be made without unreasonable delay and in no case later than 60 days from the date of discovery.
    b. If the breach involves computerized data, notification must also be made to the New York State Office of the Attorney General, the NYS Department of State Division of Consumer Protection, and

the NYS Division of State Police within 5 business days of notifying the HHS Secretary. Notice may be provided to all three entities through the Attorney General's online data breach reporting form. (https://formsnym.ag.ny.gov/OAGOnlineSubmissionForm/).

3. Media Notification
   a. If the breach involves 500 or more individuals, notices will also be sent to prominent media outlets without unreasonable delay and no later than 60 days following the discovery of the breach. The Privacy Officer will involve the Communications department as well as Senior Leadership.

If it was determined that after the risk assessment no breach has occurred:

- Crouse will not be required to notify the individual or any regulatory agencies, however an internal follow up will be done to determine such things as:
  a. What did we learn?
  b. What can we do to ensure no further damage occurs?
  c. What can we do to prevent this in the future?

Breach Log:

Crouse shall maintain a process to record or log all breaches (potential or confirmed) of unsecured PHI regardless of the number of patients affected. Investigation efforts and notifications must be fully documented and retained for a period of no less than six years. The following information should be collected and logged for each breach:

- A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
- A description of the types of unsecured PHI that were involved in the breach.
- A description of the action taken with regard to notification of patients, the media, the HHS Secretary and, if applicable, the Department of State, the New York State Division of State Police and the Office of the Attorney General.
- The results of the risk assessment.
- Resolution steps taken to mitigate the breach and prevent future occurrences.

Content of the Notice:

The notice to the affected individual(s) shall be written in plain language and must contain the following information:

- A brief description of the incident, including the date of the discovery of the breach, and the date of the breach, if known.
- The types of unsecured PHI that were involved in the breach.
- Any steps the individual should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
- Contact procedures for individuals to ask questions or learn additional information. Includes contact information for the Crouse Hospital HIPAA Privacy Officer and the following agencies if the breach involves computerized data: Health and Human Services (HHS), New York State Office of the Attorney General, the NYS Department of State Division of Consumer Protection, and the NYS Division of State Police.

Methods of Notification:

The method of notification will depend on the individuals or entities to be notified. Notification to the individual may be made by the following methods:

- Written notification by first-class mail to the individual at their last known address or, electronic mail if the individual has agreed to it.
- Written notification by first-class mail to the next of kin or personal representative if the individual is deceased.
- Insufficient or out of date contact information for the individual (including phone, email, etc.)
    - Substitute notice is not required if there is also insufficient or out of date contact information for the next of kin of personal representative
- Insufficient or out of date contact information for fewer than 10 individuals
    - Substitute notice may be provided by an alternative form of written notice, phone call or other means.
- Insufficient or out of date contact information for greater than 10 individuals
    - Substitute notice shall be in the form of a conspicuous posting on the Crouse website for a period of 90 days, or a conspicuous notice in a major print or broadcast media in the counties that the affected individuals likely reside. The notice shall include a toll-free number to call to determine whether their PHI is included in the breach. The number will remain active for at least 90 days.

Law Enforcement Delay:

Law enforcement officials may request a delay in notification if the notification may impede a criminal investigation or threaten national security. A request for delay must be documented using one of the following two methods:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice or posting for the time period specified by the official; or
- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

Business Associate Responsibilities:

A Business Associate is anyone who creates, receives, maintains or transmits PHI on behalf of Crouse Hospital. They are required to notify Crouse of any breach of unsecured PHI without unreasonable delay but no later than 60 days from the date of discovery or by the shorter timeframe specified in the Business Associate Agreement. The notice shall include the identification of each individual whose unsecured PHI has been accessed, acquired, or disclosed. The Business Associate shall promptly provide Crouse with any other available information required for the notification. Upon notification by the Business Associate of discovery of a breach, Crouse will be responsible for notifying affected individuals, unless otherwise agreed upon by the Business Associate to perform the notification.

Examples of determination for breach/no breach

1. Crouse accidentally faxes lab results to another hospital. **Is this a breach?**

    NO. The HIPAA Privacy Rule was violated; however, the disclosure may not compromise the privacy and security of the PHI. The receiving hospital is obligated under the same HIPAA rules. It must protect that patient's information just as Crouse would.

2. Crouse discloses PHI that contains the patient's name and fact that they received treatment in our Opioid

program. **Is this a breach?**

YES. The Privacy Rule was violated. There could be significant risk to the patient both reputational and/or financial. This would apply to any specialized programs.

3. Crouse discloses PHI that contains the name of the patient and fact that they received services (but not what specific services). **Is this a breach?**

   NO. Although the Privacy Rule was violated, there is a low probability of harm.

4. The Explanation of Benefits notice for a patient who received services here is mistakenly sent to the patient's employer. **Is this a breach?**

   YES. Not only is the Privacy Rule violated, there is a high probability of reputational or financial harm to that individual. This is especially significant to any specialized programs (i.e. Behavioral Health, Opioid, Oncology, etc.).

References

Federal Register Part II, Department of Health and Human Services, 45 CFR Parts 160 and 164. American Recovery and Reinvestment Act of 2009.

Health and Human Services HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414

NYS Information Security Breach and Notification Act – Section 208 of the State Technology Law & Section 899-AA of the NY General Business Law. (SHIELD Act Amendment)

Definitions

Breach: the acquisition, access, use, or disclosure of protected health information in a manner which compromises the security or privacy of the PHI

Disclosure: the release, transfer, provision of, access to, or divulging in any manner of information outside the entity holding the information

Access: the ability or the means necessary to read, write, modify, or communicate data or information; or otherwise use any system resource

Protected Health Information (PHI): individually identifiable health information that is transmitted or maintained in any form, including paper, electronic or oral

Discovery of breach: the first day on which an incident that may have resulted in a breach is known to the organization or by exercising reasonable diligence would have been known to the organization (includes breaches by organization's business associates)

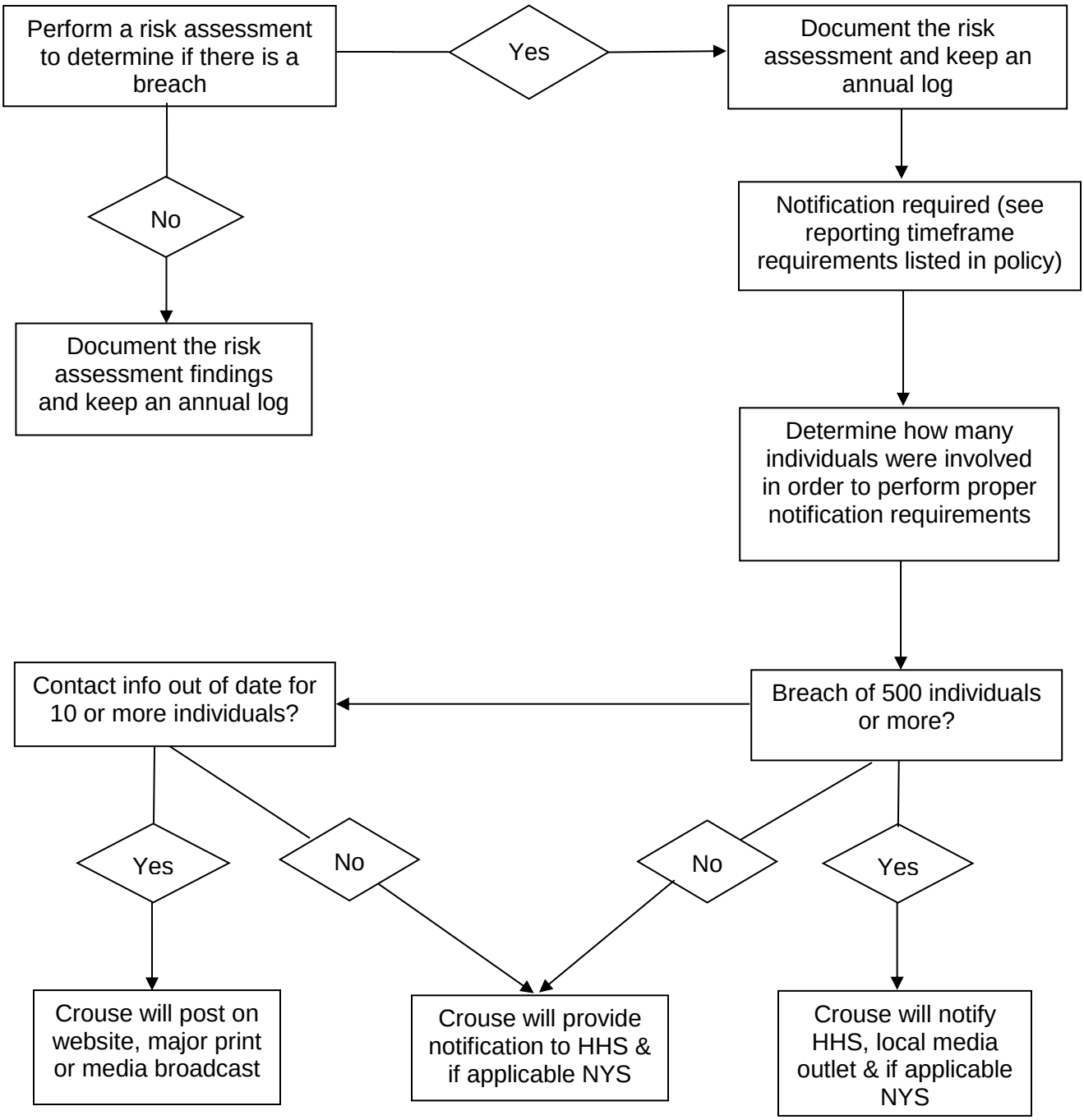
Encryption: technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals

Business Associate: a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Addendums, Diagrams & Illustrations

See Next Page

Crouse Hospital Breach Notification Process Flow Chart



736 Irving Ave
Syracuse, NY 13210

<date>
<name>
<address>

Dear _____,

This letter is to inform you that there has been a breach of your personal/health information. On __<date>__, __<description of what happened>__. __<What was involved/type of information>__.

Crouse has taken the following steps in order to investigate the breach and protect against any future breach __<list steps here>__.

In order to protect yourself from further harm resulting in this breach, __<explain steps to take>__. If you have any questions or have additional concerns you may contact the Crouse Hospital Privacy Officer at (315)470-7477. You can also write a letter to:

Crouse Hospital
Privacy Officer
Risk Management
736 Irving Ave
Syracuse, NY 13210

Sincerely,

Crouse Hospital

Information below will be added to letters for computerized data breaches.

If you would like additional information regarding security breach response and identity theft prevention and protection, please contact one of the following agencies:

- U.S. Department of Health & Human Services
  - Website: https://www.hhs.gov/
  - Phone Number: 1-877-696-6775
- New York State Office of the Attorney General
  - Website: https://ag.ny.gov/
  - Phone Number: 1-800-771-7755
- New York State Department of State, Division of Consumer Protection
  - Website: https://www.dos.ny.gov/consumerprotection/
  - Phone Number: 1-800-697-1220
- New York State Division of State Police
  - Website: https://www.ny.gov/agencies/division-state-police
  - Mailing Address: 1220 Washington Ave, Building 22, Albany, NY 12226

New York State Police Contact Information by County

Division Headquarters, Building 22, 1220 Washington Ave., Albany, NY 12226-2252		
Troop	**Phone**	**Counties in Patrol Area**
A	585-344-6200	Alleghany, Cattaraugus, Chautauqua, Erie, Genesee, Niagara, Orleans, Wyoming
B	518-897-2000	Clinton, Essex, Franklin, Hamilton, St. Lawrence
C	607-561-7400	Broome, Chenango, Cortland, Delaware, Otsego, Tioga, Tompkins
D	315-366-6000	Herkimer, Jefferson, Lewis, Madison, Oneida, Onondaga, Oswego
E	585-398-4100	Cayuga, Chemung, Livingston, Monroe, Ontario, Schuyler, Seneca, Steuben, Wayne, Yates
F	845-344-5300	Greene, Orange, Rockland, Sullivan, Ulster
G	518-783-3211	Albany, Fulton, Hamilton, Montgomery, Rensselaer, Saratoga, Schenectady, Schoharie, Warren, Washington
K	845-677-7300	Columbia, Dutchess, Putnam, Westchester
L	631-756-3300	Nassau and Suffolk
NYC	917-492-7100	New York City
T	518-436-2825	New York State Thruway