HIPAA PRIVACY BREACH INVESTIGATION AND NOTIFICATION POLICY

I. PURPOSE

To provide requirements for notification when impermissible or unauthorized access, acquisition, use and/or disclosure of an Individual’s unsecured protected health information occurs.

II. SCOPE

This policy applies to Aurora Health Care, Inc. and all its affiliates (collectively, “Aurora”) and to all Aurora employees, volunteers, contractors, students, and temporary help (collectively “Workforce Members”).

III. DEFINITIONS

Access means the act of acquiring, using, reading, writing, modifying, or communicating data/information or the ability to do so.

Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule which poses a significant financial, reputational, or other harm to the individual. The following are excluded:

- A use or disclosure of PHI that qualifies as a Limited Data Set and does not include date of birth, and zip code. (See AHC System Policy #141, Use and/or Disclosure of Protected Health Information, for the definition of Limited Data Set.)
- Any unintentional Access to PHI by a Workforce Member if such Access was made in good faith and within the scope of job duties, and does not result in further use or Disclosure in a manner not permitted under the Privacy Rule.
- Any inadvertent Disclosure by a Workforce Member who is authorized by their job duties to Access PHI, to another authorized Workforce Member, and the information received as a result of such Disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
- A Disclosure of PHI where there is a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Disclosure means the releasing, transferring, providing, sharing, or divulging in any other manner of information.

Protected Health Information” (“PHI”) means any information, whether oral or recorded in any form or medium, which relates to:

- The past, present or future physical or mental health or condition of an individual;
- The provision of health care to an individual; or
PHI includes demographic, insurance, billing, medical and other information Aurora collects, creates or receives in the course of providing health care to an individual. It includes oral information and information recorded in all media: for example, paper, electronic, film, etc. PHI excludes employment records held by Aurora in its role as an employer and certain education records.

Unsecured Protected Health Information means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued.

IV. POLICY

A. Breach notification shall be carried out by Aurora in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification laws.

B. Workforce Members shall report any potential HIPAA Privacy violation as soon as is reasonably possible to their Site Privacy Officer, Aurora's Chief Privacy Officer, or to their supervisor/manager who will then make the report. Incidents that involve observed or suspected security incidents shall additionally be reported as per the Information Security Policy #118.

C. Any harmful effect of a HIPAA Privacy Rule violation that is known to Aurora shall be mitigated to the extent practicable.

D. Following the determination that an impermissible access, use, or disclosure of PHI poses a significant risk of financial, reputational, or other harm to the individual, Aurora shall notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach. PHI that has been determined to be secure does not pose a significant risk of harm.

E. Any Aurora Business Associate ("BA") that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay notify Aurora of such breach as per the terms of the Business Associate Agreement. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide any other available information that is required to include in the notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, Aurora shall be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals. Regardless of who performs the notification, Aurora is responsible to document the notification.

F. Annual reporting to the U.S. Department of Health & Human Services for breaches involving less than 500 individuals shall be completed via the designated website prior to March of the following calendar year. Reporting of breaches involving 500 or more individuals shall occur simultaneous to the notifications to the individuals. Reporting shall be the responsibility of the Chief Privacy Officer.
V. PROCEDURE

A. Following the discovery of a potential Breach, the Site Privacy Officer or other designated Workforce Member working under the direction of the Chief Privacy Officer shall facilitate an investigation and conduct a risk of harm assessment. If a Breach is substantiated and notification is required, the Site Privacy Officer or Chief Privacy Officer shall direct and oversee the process to notify each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the Breach. The Chief Privacy Officer, in collaboration with the Public Affairs and other applicable departments as necessary, shall also direct and oversee the process of determining what additional external notifications are required or should be made (for example, Secretary of Department of Health & Human Services, media outlets, law enforcement officials, etc.).

B. Upon determination that notification is required, the notice must be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. A Breach shall be treated as “discovered” as of the first day on which such breach is known to Aurora, or, by exercising reasonable diligence would have been known.

C. If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Aurora shall:

1. 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  

2. 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.

D. Aurora shall demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay by retaining the supporting documentation. All documentation related to the investigation, risk of harm assessment, and notification shall be retained by the Chief Compliance Officer for six (6) years.

CROSS REFERENCES  
AHC System Policy #118 - Information Security  
AHC System Policy #141 - Use and/or Disclosure of Protected Health Information

OWNER  
Director & Chief Privacy Officer

REFERENCES  
45 C.F.R., Parts 160 and 164: HIPAA Privacy and Security Rules  
American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH): HIPAA Breach Notification for Unsecured Protected Health Information  
Pub. L.111-5, Section 13402(h)(2): Guidance related to unsecured PHI

REVIEW DATES