AUBURN COMMUNITY HOSPITAL &
THE FINGER LAKES CENTER FOR LIVING
17 LANSING STREET
AUBURN, NEW YORK 13021

Subject: **HIPAA & NY Shield Act Breach Notification Policy**	Policy No.: CC: 12
Department: Administration: Corporate Compliance	Page: 1 of 5
	Date Issued: 12/3/2015

I. Scope of Policy

This Policy applies to all persons affected by the organization's risk areas, including employees, the chief executive officer and other senior administrators, managers, and contractors, agents, subcontractors, independent contractors, and governing board and corporate officers of Auburn Community Hospital ("ACH") and its affiliated entities, including Auburn Memorial Medical Services, P.C. ("AMMS"), Anesthesia Group, and Finger Lakes Center for Living ("FLCL") ("Affected Individuals"), as appropriate. Note, ACH, AMMS, Anesthesia Group and FLCL are referred to collectively as "Hospital" hereunder.

II. Purpose; Definitions

i. The purpose of this Policy is to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013), which requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI; and 2) the NY Shield Act/General Business Law § 899-aa.

III. Policy

It is the policy of Auburn Community Hospital ("Hospital") to provide timely notification to patients about breaches of their PHI and PI to help reduce or prevent identity theft or fraud.

IV. Breaches of PHI

a. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. Only breaches of "unsecured" protected health information ("PHI") trigger HIPAA's breach notification requirements. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of Health and Human Services ("HHS").

b. Breach excludes:

i. Any unintentional acquisition, access, or use of PHI by a Hospital workforce member or person acting under the authority of the Hospital or its business associates, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner that violates the HIPAA Privacy Rule.

ii. Any inadvertent disclosure by a person who is authorized to access PHI at the Hospital, or its business associate, to another person authorized to access PHI at the Hospital, or its business associate, and the information received as a result of such disclosure is not further used or disclosed in violation of the HIPAA Privacy Rule.

iii. A disclosure of PHI where the Hospital or its 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.

c. Except in those situations identified above, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is **presumed** to be a breach unless the Hospital (or its business associate, if applicable) demonstrates that there is a **low probability** that the PHI has been compromised based on a risk assessment of at least the four following factors:

i. **The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification**. For example, was sensitive data, such as a patient's Social Security number and detailed clinical information, involved in an incident?

ii. **The unauthorized person who used the PHI or to whom the disclosure was made**. For example, if the disclosure was to another HIPAA-regulated entity or to a federal agency, this *may* result in a lower probability that the PHI has been compromised since the recipient of the information is obligated to abide by HIPAA.

iii. **Whether the PHI was actually acquired or viewed**. For example, this might involve a forensic analysis or investigation that could determine whether PHI contained on a lost or stolen laptop or other portable electronic device actually was viewed or accessed.

iv. **The extent to which the risk to the PHI has been mitigated**. For example, this might involve reaching out to an unauthorized recipient of the PHI to obtain satisfactory assurances (through a confidentiality agreement or similar means) that any PHI sent to a recipient was not further used or disclosed but instead destroyed.

d. With respect to a ransomware attack, HHS, Office of Civil Rights ("OCR") has provided additional guidance including other factors to consider when determining whether PHI has been compromised, including:
   i. Whether there is a high risk of unavailability of the data, or high risk to the integrity of the data;
   ii. Whether the Hospital has any contingency plans such as recovery or data back-up measures to demonstrate the ransomware has not impacted the availability or integrity of the PHI; or
   iii. Whether the data was encrypted at rest, and therefore the ransomware encrypted data that was already encrypted.
   iv. For more information and the OCR guidance on ransomware, see the Fact Sheet available at: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

V. Breaches of PI

a. Breach of a security system under the NY GBL means any unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of PI maintained by the Hospital.
   i. To determine To determine whether PI has been **accessed**, or is **reasonably believed to have been accessed**, Hospital may consider, among other factors, indications the information was:
      1. Viewed; or
      2. Communicated with; or
      3. Used; or
      4. Altered by a person without valid authorization or by an unauthorized person.
   ii. To determine whether PI has been **acquired**, or is **reasonably believed to have been acquired**, Hospital may consider, among other factors, indications that the information:
      1. Is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
      2. Has been downloaded or copied; or
      3. Was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

   iii. Breach for purposes of the NY GBL excludes any good faith access to, or acquisition of, PI by an employee or agent of the Hospital for Hospital purposes, provided that the PI is not used or subject to unauthorized disclosure.

   iv. Notification to affected persons is not required if the exposure of PI was an inadvertent disclosure by persons authorized to access the PI, and the Hospital reasonably believes such exposure will not likely result in misuse of PI, or financial harm to the affected persons, or emotional harm in the case of unknown disclosure of online credentials (such as defined in section III (c)(ii)). Such a determination must be documented (see section VII (h)(ii)).

VI. Reporting and Determination

a. All Affected Persons are expected to report any suspected breach of PHI of PI immediately to the Privacy Officer.

b. .For incidents involving PHI: After consideration of the factors under section IV (d), and if applicable section IV (e), is there a **low probability** that the PHI has been compromised? If the answer is "no", then a reportable breach has occurred (conversely, if the answer is "yes", then a reportable breach has not occurred).

a. For incidents involving PI: After consideration of the factors under section V (a), has the computerized data containing PI been accessed or acquired by unauthorized person(s)? If the answer is "no", then no breach of the security system has occurred. Conversely, if the answer is "yes", Hospital must next determine if the exposure of PI was an inadvertent disclosure? If the answer is "yes", then no notification to affected persons is required, however, Hospital must follow the documentation and notification to NY State Attorney General requirements described in section VII (h) below.

b. If a breach contains only PHI, and no PI, the Hospital must follow the procedures that follow in section VII (a)-(d) below. Note that notice to the NY State Attorney General must be made five (5) days after the Hospital provides notice to the HHS Secretary per section VII (d) (even if no PI was included in the breach).

c. If a breach contains only PI, and no PHI, the Hospital must follow the procedures in section VII (a)-(b) and (e) below.

VII. Procedure

The Hospital and its business associates, as applicable, must only provide the required notifications if the breach involved unsecured PHI. Following a breach of unsecured PHI, the Hospital must provide notification of the breach to all affected individuals, the Secretary of HHS, and in certain circumstances, to the media.

a. In addition to the procedures set forth in this policy for breach of PHI, refer to the HHS, Office of Civil Rights website for more information on breach notification requirements: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html. For additional information on breaches of PI, refer to NYS Department of State, Office of Consumer Protection website for notification requirements: https://dos.ny.gov/data-security-breach-management. Breaches can be reported through the link available from the NYS Attorney General here: https://formsnym.ag.ny.gov/OAGOnlineSubmissionForm/faces/OAGSBHome

b. **Notification to Individuals.**

i. The Hospital shall notify individuals following discovery of a reportable breach. A breach is treated as "discovered" by the Hospital as of the first day on which such breach is known to, or should reasonably have been known to any employee, officer or agent of, the Hospital other than the person who committed the breach.

ii. Notification shall occur without unreasonable delay and in no event later than 60 calendar days from discovery of the breach, unless delay of notification is authorized by law enforcement requests a delay (see Section VII(f) below). Note, however, that The NY GBL requires Hospital to send such notice "in the most expedient time possible" which suggests 60 days might be too long.

iii. Content of Notice. Breach notice must include, in plain language, a brief description of what happened, including the date of the breach and the date it was discovered; a description of the types of unsecured PHI or PI involved (e.g., full name, SSN, date of birth, etc.[1]); steps the individual should take to protect him/herself from potential harm; a brief description of the actions taken by the Hospital in response to mitigate the harm and protect against future breaches; and contact procedures for the individual to ask questions or learn additional information.

iv. First class mail shall be the default method of notification. The Hospital may use e-mail if requested by the individual. If the Hospital has insufficient or out-of-date contact information that precludes written notification to the individual, the Hospital may use substitute notice, including telephone or other means, as appropriate. In instances where there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting on the Hospital's website or local print or broadcast media to provide notice of a breach. Such notice in media or web positing will include a toll-free phone number where an individual can learn whether or not the individual's unsecured PHI is possibly included in the breach.

c. **PHI: Notification to the Media.** The Hospital shall notify major local media outlets of a breach affecting more than 500 individuals without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except in the event of a law enforcement delay as noted in Section VII(G) below. Refer to "Content of Notice" above in VII(c)(iii) for information to be included in the notice.

d. **PHI: Notification to the Secretary of Health & Human Services.**

i. Breach Affecting Fewer than 500 Individuals: The Hospital will maintain a log or other documentation of any breach affecting fewer than 500 individuals. The Hospital will provide notice of these breaches to the Secretary of HHS annually within 60 days of the end of the calendar year in which the breaches were discovered. A separate notice must be submitted electronically for every breach that has occurred

[1] Note: "types of unsecured PHI" of "PI" means a general description, not the actual specific information. For example, the Hospital would explain in the notice that a SSN or date of birth was disclosed, but would not include in the breach notification letter the actual SSN or date of birth.

during the calendar year at http://ocrnotifications.hhs.gov/. These notices may be updated with any additional information that becomes available using the same website as necessary.

ii. Breach Affecting 500 or More Individuals: Notice of a breach affecting 500 or more individuals must be provided to the Secretary of HHS **without unreasonable delay**, and **in no case later than 60 days** from the discovery of the breach, except in the event of a law enforcement delay noted in Section VI(d) below. The notice must be submitted electronically at: http://ocrnotifications.hhs.gov/

iii. Refer to the HHS website for further instructions on providing notice, including content, to the Secretary of Health & Human Services found here: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

e. **PI: Notification to NY State Entities**.

i. The Hospital must provide notice, without delay, to the NY State Attorney General, the Department of State Division of Consumer Protection, and the Division of State Police as to the timing, content and distribution of individual notices and the approximate number of affected persons. Hospital shall provide a copy of the template of the notice sent to affected persons.

ii. If more than 5,000 notifications are to be sent to NY individuals, Hospital must provide notice, without delay, to consumer reporting agencies as to the timing, content and distribution of the notices and the approximate number of affected persons.

iii. Refer to the DOS website for further instructions on providing notice, including content, to NYS authorities and consumer reporting agencies. A sample notification letter can be found here: https://dos.ny.gov/data-security-breach-notification-sample-letter

f. **Law enforcement Delay.** If a law enforcement official states to the Hospital or to our business associate that a breach notification required under this policy would impede a criminal investigation or cause damage to national security, the Hospital shall:

i. Delay such notification for the time period specified if the request is in writing; or

ii. Delay such notification no longer than 30 days from the date of the request if such request is made orally. (Note: If the request is made orally, the Hospital must document the request, including the law enforcement official's identity.)

g. **Business Associates.**

i. Business Associates of the Hospital will be encouraged to immediately report to the Hospital all suspected and/or actual breaches, losses, or compromises of PHI, whether secured or unsecured.

ii. Business Associate contracts, whether existing or new, shall include corresponding breach notification requirements.

h. Documentation.

iii. All breach-related activities and investigations shall be thoroughly and timely documented.

iv. Hospital must document any determination that exposure of PI was inadvertent, as described in section V (c) above, and must maintain such documentation for at least five (5) years. If the incident affects more than 500 NY residents, Institution must provide a copy of its written determination to the NY Attorney General within ten (10) days after the determination.

h. **Staff Training and Re-education.**

i. Re-education shall be provided to all Affected Individuals involved directly or indirectly with a breach.

ii. Affected Individuals are responsible to protect the privacy and security of our patients' PHI and for compliance with this policy. Staff may be subject to discipline up to and including termination of employment for breaches of PHI and/or violations of this policy.

Approved:	John W. Bagenski, MT(ASCP)	Corporate Compliance Officer	10/29/2024
	Name	Title	Date
Approved:	John W. Bagenski	Corporate Compliance Officer	7/16/2024
	Name	Title	Date

Revised: 12/11/2018

Reviewed: 6/15/14, 8/30/2016, 7/16/2024, 10/29/2024