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

Subject: Secure System and Application Testing Policy	Policy No.: CC: 4
Department: Administration; Corporate Compliance	Page: 1 of 5
	Date Issued: 7/25/2012

SCOPE:
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.

PURPOSE:
The purpose of this Policy is to identify the processes and practices that protect the integrity, security, and confidentiality of protected health information ("PHI") and other Confidential Information at all stages in the provision of care and testing of IT assets.

The Hospital, as a provider that electronically transmits health information in connection with certain transactions, is defined as a covered entity under HIPAA. These transactions include claims, benefit eligibility inquiries, referral authorization request, other transactions for which the U.S. Department of Health and Human Services has established standards under the HIPAA Transactions Rule, or any tests for systems, modules, and applications involved in such processes. Affected Individuals of the Hospital shall treat each instance of PHI in a test environment as though they were performing an actual transaction or transmission of health information.

POLICY:
Affected Individuals shall establish, respect and maintain the privacy, security and confidentiality of all Hospital confidential business and proprietary, clinical, patient PHI, and employee information (collectively the "Confidential Information") in compliance with applicable state and federal laws and regulations governing the privacy of such Confidential Information, including, without limitation, the Health Insurance Portability and Accountability Act of 1996 and the implementing regulations thereto ("HIPAA"). Accordingly, the protections

afforded to Confidential Information apply not only to daily operations and the provision of care, but also to the use of PHI in systems and applications testing environments. For purposes of this policy, Confidential Information, including PHI, may be in any form or media (e.g., written, electronic, video, photographic, audio, oral, etc.).

DEFINITIONS:

Protected Health Information ("PHI"): HIPAA protects all "individually identifiable health information" (defined below) held or transmitted by a covered entity (such as the Hospital) or its business associates, in any form or media, whether electronic, paper, or verbal.

Individually Identifiable Health Information: Information, including demographic data, that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) and relates to:

- The individual's past, present, or future physical or mental health or condition,
- The provision of healthcare to the individual, or
- The past, present, or future payment for the provision of healthcare to the individual.

De-Identified Health Information: De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are no restrictions on the use or disclosure of de-identified health information. There are two methods to de-identify information:

- A formal determination by a qualified statistician, or
- The removal of specified identifiers as required by HIPAA (See Section B of this policy) of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

Minimum Necessary Standard: When using or disclosing PHI or when requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

Sanitizing: As part of the National Industrial Security Program initiative, the Defense Security Services has developed the standard 5220.22-M National Industrial Security Program Operating Manual outlining the removal of PHI from unclassified hard drives, defined as sanitizing. The National Industrial Security defines this overwriting technique so that it will remove any existing data yet leave the hard drive in a state where it can be reused.

POLICY:

A. Access controls and adherence to the minimum necessary standard shall be implemented to ensure the confidentiality of the data from unauthorized use and disclosure for all instances, including in test environments.

B. Whenever possible, Affected Individuals, as applicable, operating in test environments shall remove the following data elements to help ensure the privacy and security of PHI:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and equivalent geographical codes, except for the initial three digits of a ZIP Code if, according to the currently publicly available data from the Bureau of the Census:
    a. The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people
    b. The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000
3. All elements of dates (excluding year) directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Facsimile numbers
6. Electronic mail addresses
7. Social Security Numbers
8. Medical Record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by HIPAA for re-identification

C. Where the de-identification of PHI is not possible for effectively testing the system, module, or application, the following standard must be followed:

1. Where utilizing PHI is allowed, production data must be de-identified as much as possible, without compromising the quality of the test.
2. All copies of PHI and data must be destroyed through the clearing of the environment after authorized use is completed (see Section G of this policy).
3. All testing environments must comply with all company security standards.
4. Security administration procedures must be followed for all testing environments (i.e., strict maintenance of user account privileges).
5. All standards for minimum necessary must be followed.
6. Testing with external entities is allowed only with other covered entities, unless a valid Business Associate Agreement is in place prior to testing.

7. Any data used for testing must come from the same population of data that the external entity would normally receive in production runs.

D. All Affected Individuals with access to PHI in a test environment will be subjected to annual compliance training for privacy purposes. Such training shall reinforce privacy and security concepts, including, but not limited to, the following:

1. Not sharing passwords.
2. Avoid writing passwords down on paper.
3. Reporting any security incidents.
4. Expediently and effectively managing suspected viruses.

E. Hospital Managers shall also distribute security checklists and competency tests to Affected Individuals, as applicable, and make security policies available on the Hospital's intranet, while posting updates in relevant communication channels.

F. All locations—both live and in test—where PHI is housed shall be identified and procedures shall be reviewed and updated as necessary, specifically reviewing:

1. Physical access entry controls;
2. Identification of individuals authorized to approve access;
3. Maintenance of access control lists;
4. Process for removing access for individuals no longer authorized;
5. Emergency access steps and procedures; and
6. Requirements for visitor escorts and sign-in logs.

G. Before disposing of electronic media used to host PHI at the Hospital in both test and live environments, Affected Individuals shall ensure that all sensitive data is disposed of or sanitized, including:

1. Before a sanitization product is acquired, careful analysis of overall costs associated with overwrite and sanitization processes shall be made. Depending on the environment, the size of the drive and the variability in the time to perform sanitization on the product, destruction of the media may be the more preferred sanitization method.
2. Sanitization staff shall overwrite all addressable locations with a character, followed by its complement. Affected Individuals shall verify that "complement" character was written successfully to all addressable locations, then overwrite all addressable locations with random characters, or verify third overwrite of random characters.
    i. Overwrite utility must write/read to "growth" defect list/sectors, or disk must be mapped before initial classified use and remapped before sanitization.
    ii. Difference in the comparison lists must be discussed with the Defense Security Service Industrial Security Representative and/or Information System Security Professional before declassification.

3. Note: *Overwrite utilities must be authorized by the Defense Security Service before use.*

H. The Hospital shall establish a test team leader, responsible for critical test environment operations, including:

1. Project planning, scheduling, communicating project status, and assigning and monitoring project tasks.
2. Ensuring that project plan changes are incorporated into the test plan, above and beyond writing a test plan and test strategy.
3. Identifying relevant risks and working to mitigate them.
4. At the end of project testing life cycle, ensuring that all test objectives are accomplished and acceptance criteria are met.

RELATED POLICIES
IT Security and Confidentiality Policy
IT Privileged User Access Policy
IT Security Controls Policy
IT Security Incident Management Policy
IT Security Incident Reporting Policy
IT Temporary Emergency Access Policy
Staff Nondisclosure Agreement

This policy is supplemented by other Hospital and IT policies and procedures. All IT security, HIPAA, and Joint Commission related policies are located on the Hospital's Intranet.

All IT security policies and procedures shall adhere to standards established by appropriate international conventions, Federal, State, and local laws and regulations.

Approved: John W. Bagenski, MT(ASCP) Corporate Compliance Officer 10/29/2024
Name Title Date
Revised:
12/11/2018; _9/26/2024
Reviewed:
8/30/2016. 12/11/2018, 7/16/2024, 9/26/2024, 10/29/2024