ALLINA HOSPITALS & CLINICS
System-wide Policy

Department: **Allina Hospitals & Clinics** **Corporate Compliance** **Privacy & Security Compliance**	**Policy Title:** **HIPAA Privacy & Security Documentation Standards**
Page: **1 of 6**	**Effective Date:** **April 14, 2003**
Approved by: **Ethics & Compliance Oversight Committee**	**Revised:** **January 2003; March 2003; June 2004, January 2005, June 2006; December 2006, December 2007**
Reference Number: **PSC102**	

Scope:

This policy covers the responsibilities and obligations of all Allina Business Units regarding their role in the documentation, designations, policies and procedures, and other actions required for compliance with the HIPAA Privacy and Security Regulations.

Purpose:

To provide a summary of the policies and standards of Allina Hospitals & Clinics with respect to documentation required for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Regulations.

The HIPAA Privacy and Security Regulations require that covered entities maintain documentation of certain decisions, designations, policies and procedures, and other actions taken for purposes of compliance with the regulations. The purposes of these documentation requirements are to provide a basis for workforce training, to facilitate the creation of the required notice of privacy practices, and to enhance accountability for compliance with the regulation.

Policy:

It is Allina's policy to fully comply with all documentation requirements imposed by the HIPAA Privacy and Security Regulations. Each Allina Business Unit shall:

- Develop, maintain and retain in accordance with this policy the documentation described below.

- Develop, document and implement procedures as necessary to ensure compliance with this policy.

- Provide training to appropriate personnel as necessary to ensure satisfaction of these documentation requirements.

Definitions:

Protected health information (PHI) means, generally, health information that is individually identifiable (i.e., patient-specific) and that is created, maintained, used or disclosed by or for an Allina Business Unit. More specifically, the term refers to information that:

(i) identifies or could reasonably be used to identify the individual

(ii) relates to:

(a) an individual's physical or mental health or condition
(b) the provision of health care to an individual
(c) payment for health care provided to an individual

For example, protected health information includes information that identifies an individual as an Allina patient, or that associates condition, treatment or payment-related information (diagnosis codes, dates of service, charge data, etc.) to information that could be used to identify the individual (name, other demographics, medical record number, images, etc.).

Electronic protected health information (ePHI) is PHI maintained or transmitted in electronic form. The HIPAA Privacy and Security Regulations do not distinguish between electronic forms of information. Some examples of ePHI are patient information stored on magnetic tapes or disks, optical disks, hard drives, and servers. Examples of transmission media include Internet and Extranet technology, leased lines, private networks, and removable media such as disks.

The HIPAA Security Rule defines a "security incident" as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Procedure:

1. Policies and Procedures

Policies addressing compliance with privacy and security laws and regulations will be developed in accordance with Privacy & Security Compliance Policy PSC 103, "Policy Development and Enactment." Allina's organization-wide Privacy & Security Compliance policies identify numerous topics to be addressed in Business-Unit specific policies. In addition, each Business Unit will adopt supporting procedures as provided in such policies and otherwise as necessary to enable effective policy implementation and workforce training.

The Privacy & Security Officer will provide direction and oversight to corporate human resources for development of policies specific to Allina's employee health benefit plans. Such policies may vary from the standards in Allina's organization-wide policies as necessary to reflect the differences in regulatory requirements applicable to covered entities that are health plans. Similarly, policies and procedures that address compliance for Business Units operating outside of Minnesota may vary from the organization-wide standards as necessary to reflect the requirements of other states' laws (e.g., Wisconsin).

Documented policies and procedures related to privacy and security compliance obligations will be modified promptly to comply with changes in relevant laws and regulations, and policy and procedure changes will be implemented within the time required for legal compliance.

The Privacy & Security Officer shall ensure that Allina's organization-wide Privacy & Security Compliance policies and procedures are maintained and retained in accordance with this policy. The Compliance Accountable Executive for each Business Unit, or his or her designee, shall ensure that Privacy & Security Compliance policies and procedures specific to that Business Unit are maintained and retained in accordance with this policy.

2. Notice of Privacy Practices

The Privacy & Security Officer will be responsible for developing, with all necessary input from stakeholders within operations and corporate areas, Allina's Notice(s) of Privacy Practices. The Corporate Compliance department will retain copies of the notice(s) issued as documentation of compliance.

The Privacy & Security Officer shall ensure that Allina's Notice(s) of Privacy Practices is promptly revised and distributed to Business Units whenever there is a material change to the uses or disclosures, individuals' rights, Allina's legal duties or other privacy practices described in the notice(s).

See also provisions relating to Allina's Notice(s) of Privacy Practices in Privacy & Security Compliance Policy PSC200, "Privacy and Individual Rights under HIPAA."

3. Complaints about Privacy and Security Compliance Practices

Within each Business Unit (excluding System Office areas that are not responsible for employee health benefit plans or patient billing and that do not otherwise receive individuals' complaints in the regular course of business), the designated office or person responsible for receiving complaints relating to privacy and security compliance practices will be responsible for documenting the complaints received and their disposition. See also provisions relating to complaints about privacy and security practices in Privacy & Security Compliance Policy PSC200, "Privacy and Individual Rights under HIPAA."

4. Report of Disclosures

Each Business Unit (excluding System Office areas that are not responsible for employee health benefit plans or for patient billing) will document its designation of the persons or offices responsible for receiving and acting on an individual's request for a report (or "accounting") of disclosures of protected health information. In addition, for each disclosure required to be included in a log maintained for purposes of producing such reports (or, for Business Units operating in Wisconsin, disclosures required to be documented by Wisconsin law[1]), each such Business Unit will document:

- The date of the disclosure.
- The name of the entity or person who received the protected health information and, if known, the entity or person's address.
- A brief description of the protected health information disclosed.
- A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure[2].
- Any written disclosure report that is provided to an individual.

See also Privacy & Security Compliance Policy PSC200, "Privacy and Individual Rights Under HIPAA," for more detailed policies concerning the requirement for disclosure logging and reporting and related documentation.

5. Access to Protected Health Information

Each Business Unit (excluding System Office areas that are not responsible for employee health benefit plans or for patient billing) will document the contents of the designated record set that is subject to access by individual, and the titles of the persons or offices responsible for receiving and processing requests for access. In Wisconsin, for each request by a patient (or person authorized by the patient) to inspect or copy the patient's health care records, the name of the inspecting person, the time and date of the inspection and the records released for inspection must be recorded.[3] See also provisions relating to access rights in Privacy & Security Compliance Policy PSC200, "Privacy and Individual Rights under HIPAA."

6. Amendment of Protected Health Information

Each Business Unit (excluding System Office areas that are not responsible for employee health benefit plans or for patient billing) will document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals. See also provisions relating to amendment rights in Privacy & Security Compliance Policy PSC200, "Privacy and Individual Rights under HIPAA."

[1] Wis Stat § 146.82(2)(d)
[2] Not necessary for logging required only by Wisconsin law.
[3] Wis. Stat. § 146.83(3)

7. Restriction Requests Granted

When a Business Unit agrees to honor an individual's request for a restriction on the Business Unit's use or disclosure of protected health information for treatment, payment or health care operations, the Business Unit must document the restrictions. See also provisions relating to restriction requests in Privacy & Security Compliance Policy PSC200, "Privacy and Individual Rights under HIPAA."

8. Disciplinary Action for Violations

Any time that disciplinary action is taken for violation of privacy and security policies or related procedures, the relevant manager or supervisor will ensure that such action is appropriately documented. At a minimum, such documentation will identify the disciplined workforce member, the date of the action, the nature of the violation, and the type of sanction imposed. In addition to documenting the action in the individual's personnel file (or in a central file, for workforce members such as volunteers for whom no personnel file is maintained), the manager or supervisor must provide such documentation without individual identification to the relevant Compliance Program Director to facilitate a Business Unit's response to any external inquiry. See also Privacy & Security Compliance Policy PSC402, "Responding to Privacy and Security Violations" and Human Resources Policy 600, "Employee Coaching and Discipline".

9. Business Associate Assurances

Each Business Unit must ensure that written assurances regarding privacy and security are obtained from that Business Unit's business associates in accordance with Privacy Compliance & Security Policy PSC300, "Business Associate Contracting." These written assurances must be retained as documentation in accordance the section below titled "Retention of Documentation."

10. Authorizations for Use and Disclosure

Any signed authorization for use and/or disclosure of protected health information, and any written revocation of a previously signed authorization, will be retained as documentation in accordance with this policy.

11. Research Documentation

Refer to Privacy & Security Compliance Policy PSC311, “Use and Disclosure of Protected Health Information for Research”, for policies addressing HIPAA Privacy Regulation documentation standards relating to research activities.

12. Retention of Documentation

All documentation required under this policy will be retained for a period of not less than six (6) years from the date of its creation or when it was last in effect, except for logging required by Wisconsin law, which shall be retained indefinitely. Each Business Unit will implement procedures designed to ensure that affected documentation is retained for the required period of time and that it is available as necessary to comply with the requirements of the HIPAA Privacy and Security regulations (for example, in the case of documentation to enable a timely and accurate accounting in response to an individual’s request), and to demonstrate compliance in connection with monitoring activities, audits and investigations.

References:

Policy Cross - Reference

PSC103, Policy Development and Enactment
PSC200, Privacy and Individual Rights under HIPAA
PSC300, Business Associate Contracting
PSC311, Use and Disclosure of Protected Health Information for Research
PSC402, Responding to Privacy and Security Violations
IS Policy 3800 Security Incidents Management

AHC600, Employee Coaching and Discipline
AHC601, Confidentiality

Regulatory Reference

45 C.F.R. 164.530(j) (2001)

This policy, which is reviewed annually, supersedes all prior policies of the same or similar subject except to the extent it is inconsistent with the express terms of a collective bargaining or individual agreement.