

ALLINA HOSPITALS & CLINICS
System-wide Policy

Department: Corporate Compliance – Privacy & Security Compliance	Policy Title: Minimum Necessary Standards for Information Access
Page: 1 of 4	Effective Date: January 1, 2005
Approved by: Ethics & Compliance Oversight Committee	Review Date: August 2004
Reference Number: PSC301	Revised: December 2, 2002; July 2004

Scope:

This policy applies to access to protected health information by members of the workforce of an Allina Hospitals & Clinics Business Unit. However, it does not apply to:

- access pursuant to an authorization from the individual
- access required for compliance with the standardized HIPAA transactions
- access that is required to carry out activities required by other law

This policy is not intended nor should it be construed in any way to require restrictions that impair communications in treatment settings which are necessary to enable quick, effective, high-quality care.

Purpose:

To state the policy of Allina Hospitals & Clinics concerning minimum necessary, or “need-to-know” limitations on workforce access to protected health information. Privacy and Security Regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) establish “need-to-know” standards for the access that a health care provider’s workforce has to protected health information. These restrictions require a health care provider to take reasonable steps to restrict the access that its workforce members have to protected health information to the “minimum necessary” to accomplish the intended purpose of that access.

Policy:

It is Allina’s policy to abide by all federal and state regulatory requirements for “need-to-know” or “minimum necessary” restrictions relating to protected health information. Except as this policy permits otherwise, Allina’s Business Units will limit the access their workforce members have to protected health information to the minimum necessary for the intended purpose, as described in the procedure section of this policy.

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.).

Workforce means employees, volunteers, trainees, and other persons whose work for an Allina Business Unit is under Allina's direct control, regardless of whether they are paid by Allina. "Workforce" does not include individuals who do not perform work under Allina's direct control, such as independent medical staff physicians who do not also provide administrative, management, consulting or other services to or for Allina. On-site independent contractors who perform a substantial part of their work on Allina's behalf may be treated as workforce members or as business associates, at a Business Unit's discretion.

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.

Procedures:

1. Identification of Workforce Access Needs

Each Business Unit will adopt policies and/or procedures that identify each of the following:

- the classes of persons who need access to protected health information to carry out their job duties; this includes identification of non-employees
- the categories or types of protected health information needed
- conditions under which such access are appropriate

2. Limitations on Workforce Access

Each Business Unit will also implement reasonable controls for limiting workforce access to protected health information. These controls will limit access to only the protected health information a workforce member needs to carry out his or her job duties.

Reasonable controls for limiting workforce access may include:

- procedural controls (policies and procedures, training, monitoring and enforcement)
- physical controls (locks, keys, screens, etc.)
- technical controls (access logs, unique logins, passwords, application security, etc.)

3. Access to the Entire Medical Record

For activities that involve workforce access to an individual's entire medical record (as defined by the Business Unit), Allina is required to specifically identify the need for such access and state a justification. Except where a Business Unit policy or procedure states otherwise, Allina considers access to an individual's entire medical record to be reasonably necessary for at least the following activities:

Purpose	Justification(s) for Access to Entire Record
Treatment of the individual	Enables quality care, promotes patient safety

Activities relating to documentation concerning treatment of the individual or payment for care provided to the individual, including information management	Ensures accurate and complete documentation, facilitates treatment and payment, facilitates timely response to patient requests
Training of students in an accredited healthcare training program	Allows for effective training of clinical staff
Response to patient requests (release, access, amendment, etc.)	Allows for timely, accurate response to medical record-related patient requests
Accreditation activities	Permits full response to requests for records in accreditation reviews
Quality activities, including credentialing and peer review	Enables robust and comprehensive quality programs
Utilization management	Allows for effective and comprehensive utilization management
Supervision of workforce involved with treatment or documentation	Allows for discharge of supervisory duties through comprehensive oversight of workforce
Regulatory compliance activities (monitoring, auditing, etc.)	Permits comprehensive compliance oversight
Response to court order or other legal mandate, activities relating to regulatory reviews, deposition preparation	Enables compliance with legal mandates for disclosure from the medical record and other legal mandates
Internal investigations	Permits sufficiently comprehensive reviews of reported incidents, complaints or concerns
Legal review and representation, risk management	Enables attorneys and risk managers to adequately represent Allina's interests or manage the organization's risk relating to actual or potential claims

For other circumstances in which access to the entire medical record is necessary, Business Unit policies and/or procedures will state that fact and include a justification.

References:

Policy Cross - Reference

AHC601- Confidentiality
PSC600, Protection of Patient Privacy: Technical Safeguards
PSC601, Information Systems Access Management and Review

Regulatory Reference

45 C.F.R. 164.502(b), .514(d) (2001)