

Section:	Management of Information
Policy Name:	Privacy Policy to Ensure Confidentiality of Patient and Organizational Information
Scope:	System
Number:	IM.02.01.01
Date:	October 2001 (Rev. 4/03, Reviewed 1/08, Amended 7/11)

Purpose

To protect the right of confidentiality of all patients, employees, physicians and the hospital itself by limiting disclosure of confidential information to those having a **need to know in order to perform the duties of their job** or take action upon that information.

Policy

Eligibility:

EVERY Allegiance Health employee, volunteer, student, contract worker, affiliates' employee, and medical staff members and their employees have the responsibility to maintain confidentiality. In addition, any student sponsors and sponsors of contract workers are responsible for the enforcement of this policy and for addressing violations appropriately with these workers.

Guidelines:

Much of the information you come in contact with is to be considered confidential and may only be disclosed when the use of this information is needed to perform job duties. Confidential information comes in many forms and from several sources. It can be generated from the medical record, the computer system; computer generated reports, hospital correspondence, conversations, and normal daily operations. Information from the above sources may only be accessed and discussed if the information is required to perform job duties. Under no circumstances may the above resources be accessed for personal or non-work related activities or for curiosity.

Examples:

The following are examples to help ensure privacy and confidentiality:

Verbal Communications

- Patient information should not be discussed where others can overhear the conversation, e.g. in hallways, on elevators, in the cafeteria, on the shuttle buses, on any form of public transportation, at restaurants and social events.
- Dictation of patient information should occur in locations where others cannot overhear, as much as our facility allows for.

Written Information

- Confidential papers, reports, and computer printouts should be kept in secure areas. Please use your best judgment to determine what provides a secure environment in your work area.
- Confidential papers should be picked up as soon as possible from copiers, mailboxes, conference room tables and other publicly accessible locations.

Section:	Management of Information
Policy Name:	Privacy Policy to Ensure Confidentiality of Patient and Organizational Information
Scope:	System
Number:	IM.02.01.01
Date:	October 2001 (Rev. 4/03, Reviewed 1/08, Amended 7/11)

-
- Confidential papers should be appropriately disposed of, e.g. shredded or deposited into the designated recycling and confidential containers. These confidential containers must either be locked or maintained in a locked area and not accessible by the public, patients, or visitors.
 - Fax machines are the least controllable technology when one transmits patient information. Please refer to the policy titled **Transmitting or Receiving Personally Identifiable Health Information (Protected Health Information) via Printer or Facsimile (FAX)**, available on the Intranet under Management of Information.

Computerized Information

- Protecting your computer/smartphone/tablet access whether it is a unique logon and/or your security code is important to maintain privacy, confidentiality and your accountability for access to our systems. Please refer to policy **User Account and Password Policy, Smartphone/Tablet Usage and Access Policy** and the **Security Code Procedure for Application Access policy**. All of these policies are available on the Intranet under Management of Information.

Employee Conduct

- Workforce members with access to information about patients, employees, or business matters may only obtain information that is necessary for their job functions. Regardless of the format in which this information is obtained, i.e., verbal, written, or electronic, it must be treated with the same level of confidentiality.

The following represent some examples of, but are not limited to, **situations, which violate confidentiality when accessed or discussed for personal or non-work related purposes, or violate the patient's right to privacy.**

1. Looking up any results (lab, x-ray, etc.), census information, or admission/discharge activity for or about a co-worker, relative, neighbor, or you without a business need to know.
2. Accessing any information other than what is required to do your job is a violation of this policy, even if you don't tell anyone else. All electronic systems are monitored and audited to ensure compliance.
3. Discussing specifics of patient care in public places such as the elevator or in the hallway. Remember patient care should never be discussed outside of the capacity of doing your job.
4. Accessing medical or financial records for curiosity whether it belongs to a patient, a co-worker, or you. It is unacceptable to look up data, e.g., a friend's birthday, address



Allegiance Health Policy and Procedures

Section: Management of Information
Policy Name: Privacy Policy to Ensure Confidentiality of Patient and Organizational Information
Scope: System
Number: IM.02.01.01
Date: October 2001 (Rev. 4/03, Reviewed 1/08, Amended 7/11)

Page 3 of 5

-
- or phone number. Accessing your personal medical record requires proper authorization through Health Information Management or your physician.
5. Confirming the presence of a patient in Behavioral Health or the Secure Unit.
 6. Giving information gathered during job duties to those with no need to know this information.
 7. Disclosing confidential information overheard or seen while performing job duties.
 8. Disclosing patient billing information.
 9. Disclosing other employee personnel information regarding disciplinary proceedings, compensation and benefits, etc.
 10. Disclosing peer review, quality/risk management activities, credential files, or malpractice/legal documents and variance reports.
 11. Discussing patient information with other healthcare practitioners in the course of work without using discretion to ensure that others who are not involved in the patient's care cannot overhear such conversations.
 12. Failure to knock on a patient's door before entering the room.
 13. Failure to use cubicle curtains when it is appropriate.

Violations of the Confidentiality Policy

1. A violation of this policy may result in disciplinary action up to termination.
2. A violation of this policy may result in sponsor notification, and the revoking of privileges at Allegiance Health.
3. Improper release or disclosure of information is considered a misdemeanor pursuant to Michigan Compiled Law (MCL) 750.410. Violators of this law may be subject to civil and/or criminal prosecution.
4. HIPAA - Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191). HIPAA protects a patient's privacy and confidentiality. Dissemination of their "personal identifiable information" is protected. At Allegiance Health, compliance with HIPAA regulations will be strictly monitored and enforced. HIPAA stipulates significant financial penalties and/or imprisonment for violations. These penalties are applicable to all Health Care Employees employed at Allegiance Health, our affiliates and their employees.
5. Upon separation of employment with Allegiance Health or an affiliate, any confidential information that was accessed as a necessity of your employment will



Allegiance Health Policy and Procedures

Section: Management of Information
Policy Name: Privacy Policy to Ensure Confidentiality of Patient and Organizational Information
Scope: System
Number: IM.02.01.01
Date: October 2001 (Rev. 4/03, Reviewed 1/08, Amended 7/11)

remain confidential. You can be held accountable for inappropriately disclosing this information.

Confidentiality Statement

1. All eligible people defined in this policy shall sign a Confidentiality Statement indicating acceptance and support of this policy and any departmental specific policy at their normally scheduled competency review.
2. All eligible people defined in this policy shall electronically sign the confidentiality statement when accessing the main hospital computer system once per day for each day the system is accessed.

Reporting Violations

It is the responsibility of all eligible people defined by this policy to report to a supervisor, human resources representative, or the Allegiance Health Corporate Compliance Officer any breach of confidentiality that is witnessed.

Breaches of privacy and confidentiality can be reported to the Corporate Compliance Officer anonymously at (517) 841-7850. All reported concerns brought forth in good faith shall be protected from disclosure and no employee shall fear retaliation by bringing a concern to the Corporate Compliance Officer.

Approvals:

- | | | |
|----|---|-------------|
| 1. | <i>Signature on File</i> | 7-26-11 |
| | Rick Warren, VP Information Systems & CIO | Date |
| 2. | <i>Signature on File</i> | 7-28-11 |
| | John Hyden, Corporate Compliance Officer/Privacy Officer | Date |

Author(s):

Jeanne Wymer, HIS Project Manager
Brenda K. Ruelas, Security Analyst
Hospital Confidentiality Committee

1/4/08 - Reviewed and no substantive change needs to be made at this time.

Maribeth Coulombe, Privacy Officer & Associate Legal Counsel

7/13/11 – Amended

John Hyden, Corporate Compliance Officer

