Status **Active** PolicyStat ID **11064722**

Origination	2/9/2021
Last Approved	1/25/2022
Effective	1/25/2022
Last Revised	1/25/2022
Next Review	1/25/2023
Owner	Renee Fraser
Area	Human Resources
Applicability	Gundersen
References	Policy

Confidentiality and Security of Information, HR-205

References

HIPAA, The Joint Commission, 45 CFR §164.501, Wis. Stat. § 51.30, DHS 92

Applicable To

All employees, students, Board of Directors and volunteers of Gundersen Health System, its principal affiliates, Gundersen Clinic, Gundersen Lutheran Medical Center, Inc., Gundersen Lutheran Medical Foundation, Inc., and Gundersen Lutheran Administrative Services, collectively GUNDERSEN.

Purpose Statement

It is the policy of GUNDERSEN to respect and protect the right to confidentiality and privacy of all patients and Employees concerning their Protected Health Information, Personal Information, or Employment Information. All Employees are responsible to maintain the confidentiality of this information protecting it against loss, defacement, tampering, access, or use by unauthorized individuals.

Passcodes are required for all personal mobile devices, including smart phones, tablets, iPads or other mobile devices that are used for access to corporate information, including but not limited to email or the electronic medical record. Patient related photos cannot be stored on mobile devices such as smart phones, iPads or tablets due to HIPAA regulatory requirements, and must be stored in the electronic medical record. Employees using their personally owned device for access to work-related systems, including email, are also responsible for configuring the encryption setting on the device to minimize the risk of breach of Confidential Information.

Information Systems has record of all mobile devices that connect to Gundersen Health information systems and Information Systems has the authority to remotely wipe a personal device if there is a risk

to the security of the device (i.e. Evidence of hacking or lost/stolen devices). All lost or stolen devices should be reported immediately to the Help Desk to ensure that risk mitigation steps are taken to prevent loss Confidential Information.

Definitions

Employee: All GUNDERSEN medical staff, associate staff, nursing staff, other employees, volunteers, students, instructors, and independent contractors.

Confidential Information: Verbal communications, written records, computer-based information, other electronic, visual or digital media, photographs and films, and observations, including but not limited to:

- ***Individually Identifiable Health Information:*** Information, including demographic information, that is created or received by a health care provider, health plan, or employer and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. The information either identifies the individual or presents a reasonable basis to believe the information could be used to identify the individual.
- ***Protected Health Information:*** Individually Identifiable Health Information which is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.
- ***Treatment Records:*** include all records that are created in the course of providing services to individuals for mental illness, developmental disabilities, alcoholism, or drug dependence.
- ***Personal Information:*** Patient birth date, social security number, address, phone number, admission and discharge dates, appointment or visit dates, doctors' names, family or social information, financial information.
- ***Employment Information:*** Employee address, birth date, social security number, telephone number, personnel file, job application, performance appraisal, discipline, termination, investigations, compensation and benefits.
- ***Business Information:*** Confidential business information is information of a proprietary nature related to the operations, finances, marketing or strategic plans, or internal performance measurement of GUNDERSEN. Proprietary information obtained through verbal or written internal communication is ***confidential*** unless it is made public through Administration or Marketing Services. Such information may include ***but is not limited to*** trade secrets, pricing strategies, market penetration information, marketing or promotional plans, Employee recruitment or retention strategies, quality or satisfaction ratings, patient/customer complaints or feedback, or terms of contracts.

Implementation

A. **Authorized Users of Confidential Information:**

1. Authorized Users of Protected Health Information and Personal Information include those Employees who have a **job-related need-to-know** and are:

a. Providing direct care and treatment to the patient, or

b. Required to use Protected Health Information or Personal Information to perform their assigned job responsibilities or to meet legal, regulatory, or other operational obligations of GUNDERSEN, or

c. Specifically authorized by the patient to have access to their Confidential Information, unless the Confidential Information includes Treatment Records which is governed below by Section A(2).

d. Performing research activities as outlined in policy, GL-5805: Protected Health Information, Use or Disclosure of for Research.

2. Authorized Users of Treatment Records include those Employees who have a **job- related need-to-know** and are:

   a. A health care provider who is directly involved with the patient's care and the access is necessary for the current treatment of the patient, or

   b. Required to use Treatment Records to perform their assigned job responsibilities or to meet legal or regulatory obligations of Gundersen, or

   c. Specifically authorized in writing by the patient to have access to his/her Treatment Records.

3. Authorized Users of Employment Information include those Employees who have a **job-related need-to-know** and are:

   a. Specifically authorized by an employee to have access to his/her Employment Information, or

   b. Responsible for hiring, discipline, evaluation, or termination of an employee, or

   c. Responsible for responding to employment-related complaints, e.g., grievances, discrimination, harassment, etc., or

   d. Required to use Employment Information to accomplish their job responsibilities, meet business case needs, or meet legal or regulatory obligations on behalf of GUNDERSEN.

B. **Access to Protected Health Information:**

1. The GUNDERSEN patient health care record encompasses all records related to the health and treatment of the patient prepared by or under the supervision of a health care provider. It includes paper and computer-based information and other electronic, visual or digital media from inpatient, outpatient, and emergency care. The health care record is the property of GUNDERSEN and is maintained for use by the Hospital, Clinic, and Medical Staff and for the benefit of the patient. The health care record will be maintained in secure environments within the jurisdiction and safekeeping of GUNDERSEN.

2. Access is provided to GUNDERSEN employees meeting the definition of Authorized Users and based on their **job-related need-to-know** as defined above. Refer to GL-2007, Access to GUNDERSEN Information Systems and Networks, for further guidance.

3. All information generated or handled, whether paper-based, computer-based or other electronic, visual or digital media is considered the property of GUNDERSEN. This information may not be physically removed from any GUNDERSEN facility or transmitted over the Internet to personal media without Administrative Director or Vice President approval and reasonable security measures in place. Employees will take the utmost care to protect the privacy and confidentiality of Protected Health Information and confidential, business sensitive, or GUNDERSEN proprietary information in their possession or stored on organizational or personally owned Personal Digital Assistants (PDA), cellular or smart phone devices. Refer to GL-2000, Remote Access; GL-2025, Personal Digital Assistants (PDA); GL-2004, Cellular Phones; and GL-2034, Use of Personal Cellular and Smart Phone Devices for further guidance.

4. Contact the Legal Department at ext. 56619 if you receive a court order or subpoena requesting Confidential Information.

C. **Employees as Patients:**

1. Employees are, on occasion, GUNDERSEN patients. It is imperative that GUNDERSEN employees are afforded the same confidentiality as all other patients. Access to Protected Health Information and Personal Information is limited to ***Authorized Users,*** based on their ***job-related need-to-know.***

    a. Except where allowed by law, the employee/patient's informed consent to disclose information must be obtained. Requests shall be directed to the Release of Information Office in the Health Information Management Department (HIM).

2. Employees who have access to GUNDERSEN's electronic medical record may access their own personal health care record. Employees who are not Authorized Users of Epic, CWS or Resolute will make requests for access to their personal health care record through the Release of Information Office in HIM. All employees may also access portions of their health care record through MyCare, GUNDERSEN's Patient Portal.

3. Employees ***may not*** use the electronic record to review the Protected Health Information of their children, spouses, family members, or any other person for whom they may be the appointed personal representative or guardian. Such requests must be processed through the Release of Information Office in the HIM Department. With written authorization from the patient, personal representative, or guardian, you may review the paper chart only, not the electronic record.

4. All activity within GUNDERSEN's electronic medical records is electronically tracked, leaving an audit trail linked to the employee's User ID and password.

5. Employees may not access their own billing account information Resolute within Epic. Such requests must be made through Revenue Cycle.

D. **Disclosure of Protected Health Information:**

1. While the health care record is the property of GUNDERSEN, the patient generally has control over the disclosure of information from the record.

2. Employees may be asked to provide information about a patient's health care to others. Patient Protected Health Information is confidential. You ***may respond only*** when providing

this information is ***part of your assigned job responsibility and*** you have:

a. the patient's authorization to disclose the information, ***or***

b. authorization to disclose the information by state law, federal law, or GUNDERSEN policy. Consultation with the Legal Department is recommended if there is any question regarding authorization under state or federal law to disclose Protected Health Information.

3. When it is ***not part of your job to disclose Confidential Information,*** refer the requester to the Release of Information Office in HIM.

4. If the request is from the news media, refer the requester to the Emergency Services Department (Formerly the Trauma & Emergency Center) or the Corporate Communications Department. (See Policy GL-5800). Treatment Records may not be disclosed to the news media without written consent from the patient.

5. Telephone inquiries are to be handled with discretion. Verify the identity of the caller using two methods of identification and determine whether the caller is authorized to receive Protected Health Information about the patient. If an employee has any concern regarding the identity of the caller, the circumstances of the request, or whether disclosure is permitted, the request should be referred to the employee's manager or HIM. Information should be disclosed only when the conditions outlined above are met.

E. **Disclosure of Employment Information:**

1. All inquiries and requests for Employment Information related to job applicants or current and former employees, must be referred to the Human Resource Service Center for response. (See Policy HR-125)

2. Disclosure of Employment Information to a third party will not be processed without express written authorization signed by the requesting employee.

F. **Disposal of Confidential Information:**

1. Patient healthcare records are maintained and disposed of as outlined in Policy GL-6022, Record Retention, Hospital/Clinic Patient Healthcare Records.

2. All paper materials containing Protected Health Information or employee identification or other Confidential Information shall be placed in designated confidential collection containers that are picked up for shredding on a regular basis.

3. All non-paper items containing patient or employee identification shall be sent off site for incineration in the regular waste stream. Before placing these items into the regular waste container, obliterate the person's identification, e.g., by tearing off the label, using a black marker, or destroying the diskette or CD.

4. Applicant and Employment Information shall be destroyed based on relevant legal guidelines. Such information shall be destroyed by tearing into quarters or depositing in designated confidential containers for disposal.

G. **Investigation and Discipline:**

1. Employees who become aware of unauthorized access or inappropriate handling, use, sharing, or disclosure of Confidential Information shall contact the Legal Department by calling ext. 56619. Employees who wish to report actual or suspected violations of this policy anonymously may do so by calling the Compliance Hotline (608) 784-0477 or Toll Free 1-877-532-8879.
2. Patients who believe that their Confidential Information has been accessed, reviewed, disclosed or handled inappropriately shall be referred to the Legal Department at ext. 56619.
3. The Legal Department, HIM, and Human Resource Operations Manager shall investigate each alleged breach of confidentiality.
4. Violations of this policy may result in disciplinary action up to and including termination of employment.
5. Protected Health Information is protected by state and federal law. Employees who inappropriately access, use, or disclose Protected Health Information may be personally subject to civil and/or criminal penalties.

Responsibilities

Health Information Management and Information Systems:

- Assists the Legal Department in investigations of alleged breaches of patient confidentiality by conducting audit trails.

Human Resources:

- Retains signed Confidentiality Statement forms.
- Responds to inquiries and requests for Employment Information.
- Assists the Legal Department in investigations.
- Assists and advises managers on disciplinary actions up to and including termination of employment.

Legal Department:

- Investigates all breaches of confidentiality and resolves all complaints regarding unauthorized or inappropriate access, use, or disclosure of Confidential Information.
- Advises Human Resource Operations Manager on disciplinary actions required due to violations of this policy.
- Defends GUNDERSEN in legal and regulatory proceedings resulting from violations of this policy.

Employee:

- Maintains the confidentiality of Protected Health Information, Personal Information, Employment Information, and Business Information.

- Annually acknowledges that they have reviewed and understand GUNDERSEN Policy HR-205, Confidentiality and Security of Information.
- Contacts the Legal Department if he or she becomes aware of unauthorized access or inappropriate handling, use, disclosure, or sharing of Confidential Information.

Attachments

Confidentiality Statement

Approval Signatures

Step Description	Approver	Date
General Counsel	Daniel Lilly: General Counsel	1/25/2022
Chief Human Resources Officer	Mary Mccartney: Chief Human Resources Officer	1/25/2022
Director	Linda Seubert: Director, Information Systems Security	1/25/2022
	Renee Fraser: Director	1/24/2022