MedStar Georgetown University Hospital

Title:	Policy Number:
CONFIDENTIAL PATIENT INFORMATION AND PATIENT PRIVACY	456
Issued:	**Page:**
August 1, 1980	1 of 7
Last Reviewed: September 25, 2012	
Last Revised: September 24, 2013	**Attachment:** A and B

POLICY:

It is the policy of MedStar Georgetown University Hospital to respect the right of the patient, within the limits of law, to personal privacy and confidentiality of information. The medical record is the property of MGUH and shall be maintained to serve the patient, the healthcare providers, and the institution in accordance with legal, accrediting, and regulatory agencies. Access to the medical record is governed by the procedures outlined below.

DEFINITIONS:

Access
The ability to view, obtain, edit or delete information in an electronic resource.

Authorization
Process of giving individuals access to system features and capabilities based upon their identity.

Confidential Information
Any or all Protected Health Information

Medical Record
A compendium of information in paper, microfilm, and electronic media about an individual patient during the course of his/her treatment at MedStar Georgetown University Hospital. This policy applies to all medical information regardless of medium as well as *Hospital Policy # 410 General Use and Disclosure of Protected Health Information*

Mental Health Record
Any information about a patient receiving psychiatric treatment. This information may only be released upon written authorization from the patient, or as otherwise permitted by law.

Privileged Provider
A Licensed Independent Provider (LIP) granted privileges by the Board of Directors to practice at MedStar Georgetown University Hospital or its off campus sites.

Protected Health Information (PHI)
Information created or received by MGUH that relates to past, present or future physical or mental health or condition of the individual; the provision of healthcare to an individual or the past, present or future payment for the provision of health care to an individual that identifies or could identify an individual. Any one of the following items about a patient, patients' relatives, employers or household members is defined as a direct identifier:

- Names
- Postal address information other than town, city, state and zip code
- Social Security Numbers
- Medical Record Numbers
- Account Numbers
- Certificate/license numbers
- Telephone numbers
- Fax numbers
- E-mail addresses
- Device identifiers and serial numbers
- Vehicle identifiers and serial numbers including license plate numbers
- Biometric identifiers such as finger prints or voice prints
- Full face photographic images or comparable images
- URLs (Web Universal Resource Locators)
- IP addresses
- Health Plan beneficiary numbers

Purpose Based Access
Means access and use that is permitted only because the nature of the intended access or use. Therefore even though an individual may have access to a system due to their role, they may not access a system; unless they also have a permitted purpose for accessing the system.

Role-Based Access
Access and use that is permitted based on one's roles or responsibilities with the organization.

Secondary Records
Records such as indices and all other individually identifiable patient health information maintained at MedStar Georgetown University Hospital are subject to this policy.

Substance Abuse Record
Any information about a patient receiving treatment for substance abuse. This information may only be released upon written authorization from the patient.

User
Any Hospital employee, privileged provider, student, volunteer or contractor authorized to access patient related information in an electronic information system

Workforce Member
Employees, independent contractors, volunteers, trainees and other persons whose conduct, in the performance of work for MGUH is under the control of MGUH, whether or not they are paid.

PROCEDURE:

I. **Confidentiality Compliance**

A. All workforce members and privileged providers engaged in the collection, handling or dissemination of PHI shall be specifically informed of their responsibility to protect patient data and of the penalty for violation of this trust. Violation of confidentiality of patient information shall be cause for immediate termination of access to further data, and/or immediate termination of employment and/or privileges at MedStar Georgetown University Hospital. In addition, the individual may be subject to sanctions and criminal fines under Federal regulations. (see Section VIII)

B. Workforce members and privileged providers are not to access, use, or disclose their own medical records or the medical records of any other employee, family member, neighbor, friend, acquaintance, VIP or celebrity, etc for **personal purposes**. Violation shall be cause for immediate termination of access to further data, and/or disciplinary action up to and including immediate termination of employment and/or privileges at MedStar Georgetown University Hospital. In addition, the individual may be subject to sanctions and criminal fines under Federal regulations. (see Section VIII). Workforce members and privileged providers, like all patients, must use the same procedure that patients use to access their own medical records as outlined in ***Policy #410 General Use and Disclosure of Protected Health Information.*** Workforce members and privileged providers, like all patients, may access approved patient portals for personal care related information

C. All workforce members and privileged providers will take appropriate administrative, technical and physical safeguards to protect the privacy of PHI from any intentional or unintentional use or disclosure that is in violation of the standards and requirements of the HIPAA Privacy Rule to include:

1. Never leaving PHI unattended in public areas
2. Locking patient record rooms or cabinets containing patient records
3. Use of paper shredders to dispose of PHI
4. Never disposing of PHI in an unsecured trash container
5. Never removing PHI from MGUH without permission of the Director of Health Information Management or Clinic Administrator
6. Limiting public access to fax and copy machines
7. Not discussing patient information in elevators or hallways
8. Keeping voices low when discussing patient information
9. Being aware of surroundings when using cellular phones
10. Limiting public traffic near areas where medical records are kept
11. Turning charts towards the wall so that patient identifiable information is not visible
12. Not leaving x-rays unattended on a light board

13. Using minimal information on patient whiteboards

14. Never sharing computer log-in passwords and logging off applications when leaving a computer terminal.

D. Workforce members and privileged providers may have role-based access to PHI but need to be clear about having permitted access to PHI.

E. This policy shall be made known to all employees at the time of employment. Each employee shall indicate understanding of this policy through a signed statement as part of his/her departmental orientation (***Attachment A*****).** The signed statement will be maintained in the employee's departmental personnel record. For purposes of this policy, employees include faculty, residents, staff, volunteers, and Georgetown University employees who require access for patient care purposes. Students shall sign the Confidentiality Statement for Students (***Attachment B***).

F. MGUH will train all members of its workforce, including employees and volunteers, and privileged providers on the policies and procedures with respect to PHI, as necessary for the workforce members and privileged providers to carry out their functions.

II. Confidentiality of Mental Health Records

Release of mental health information from patient records will be allowed only in accordance with the requirements of the District of Columbia Mental Health Information Act of 1978.

III. Access to Medical Records by Authorized Individuals

A. Medical records shall be available for use within the facility for direct patient care by all staff involved in the care and treatment of the patient.

B. Direct access to patient medical records for routine administrative functions, including billing, is only permitted when in strict accordance with the work assignment and when the employees have signed the confidentiality statement.

C. Direct access to patient medical records after discharge for patient care-related functions, such as quality improvement and utilization management is only permitted when in strict accordance with the work assignment.

D. Medical records shall be made available for research to individuals who have obtained approval for their research projects from the Institutional Review Board and the Vice President, Medical Affairs of the Hospital. Research projects that involve use of medical records shall be conducted in accordance with institutional policies on use of medical records for research. (See Policy #130 Human Research)

E. Access to areas housing medical records shall be limited to Medical Records personnel. The sole exception to this policy shall be the individual designated by the Director of Medical Records for access at times when the Department is not staffed. Medical records must be available and accessible at all times for patient care.

F. If photocopies or facsimiles of the medical record or portions thereof are provided to authorized internal users, the same policies/procedures and controls regarding access and confidentiality of the original document apply. Wherever possible, internal users will be encouraged to use the original medical record rather than to obtain a facsimile or photocopy.

IV. Requests for Information Contained in the Medical Record

See Policy 410 "General Use and Disclosure of Protected Health Information"

V. Reporting of Suspected or Known Breaches, Investigation, Mitigation and Sanctions

A. Any suspected or known breach of PHI that is in violation of MedStar Health and/or MGUH's HIPAA Privacy and Security policies and procedures, the HIPAA Privacy or Security Rule, or other applicable law must be reported to the MGUH Privacy Liaison or the MedStar Privacy Officer. Reporting will include:

1. Complaints and concerns raised by individuals and workforce members;

2. Suspected or known violations of MedStar Health/MGUH privacy policies and procedures

3. Suspected or known violations of business associates; and

4. Suspected or known breaches of unsecured PHI.

B. The MGUH Privacy Liaison or MedStar Health Privacy Officer will conduct an investigation in accordance with Policy 458 Incidental Disclosure and Notification of Breaches of Unsecured Protected Health Information.

C. MGUH will mitigate, to the extent practicable, any known harmful effect of a use or disclosure of PHI in violation of its policies and procedures made by any MGUH workforce member, business associate, or other responsible individual.

D. MGUH will sanction members of its workforce who fail to comply with privacy policies up to and including termination.

1. Sanctions do not apply to whistleblowers, to workforce members who are crime victims, or to individuals protected from retaliatory acts or intimidation. (See Section VI)

2. The MGUH Privacy Liaison will document any sanction applied and retain the documentation for six years

3. The MGUH Privacy Liaison must report any applied sanction for a privacy violation to the MedStar Privacy Officer

VI. Whistleblowers and Workforce Member Crime Victims

A. If a workforce member or a business associate believes in good faith that MGUH has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by MGUH potentially endanger one or more individuals, workers, or the public, the workforce member or business associate may disclose relevant patient PHI to:

1. A health oversight agency or public health authority authorized by law to investigate the conduct or conditions;

2. An appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet the professional standards or misconduct;

3. An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining legal options;

B. If a workforce member is the victim of a criminal act, he/she may disclose relevant PHI to a law enforcement official, provided that:

1. The PHI disclosed is about a suspected perpetrator of the criminal act; and

2. The PHI disclosed is limited to:

a. Name and address
b. Date and place of birth
c. Social Security Number
d. ABO blood type and Rh factor
e. Type of injury
f. Date and time of treatment
g. Date and time of death (if applicable) and
h. Description of distinguishing physical characteristics

VII. **Refraining from Retaliatory Acts or Intimidation**

MGUH will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals:

A. For filing a complaint with the Secretary of the Department of Health and Human Services;

B. Testifying, assisting, or participating in an investigation, compliance review, hearing or proceeding about an alleged violation of the HIPAA Privacy or Security Rule;

C. Opposing any act or practice that the individual believes in good faith is in violation of the HIPAA Privacy or Security Rule and the manner of the opposition is reasonable.

VIII. **Compliance Reviews and Investigations**

A. Periodic Privacy Compliance Reviews
In coordination with MedStar's Privacy Officer, the MGUH Privacy Liaison will conduct periodic privacy compliance reviews at MGUH.

B. Investigation and/or Privacy Compliance Review by the Department of Health and Human Services (DHHS)

1. The MGUH representative should immediately contact the MGUH Privacy Liaison, MedStar Privacy Officer and Legal Services upon notification of a compliance review or an investigation by the DHHS.

2. MGUH must cooperate and provide records and compliance reports as requested by DHHS.

3. MGUH will permit DHHS to access information that is pertinent to ascertaining compliance with the HIPAA Privacy Rule.

    a. During normal business hours, such access will be provided to MGUH's facilities, books, records, accounts, and other sources of information; or
    b. At any time and without notice, such access will be provided if DHHS determines that exigent circumstances exist.

4 MGUH must certify and document efforts made to obtain information required by the DHHS that are in the exclusive possession of any other agency, institution or person and they fail to produce the information.

_____

Richard L. Goldberg, M.D.
President

Related Policies: 130 Human Research
402 Release of Information to the News Media
410 General Uses and Disclosure of Protected Health Information
457 Patient Privacy Rights