

Confidentiality

All hospitals within the Partners HealthCare network are committed to providing patients with high quality health care and to forming relationships with them that are built on **trust**. That means respecting the **privacy** and **confidentiality** of each patient's health information. We tell patients that we protect their privacy and confidentiality rights by creating and putting into practice policies and procedures that allow hospital employees to access to their personal medical information only for legitimate reasons.

Major Points:

- 1. Need to Know.** Access to confidential information without a patient care/business need-to-know in order to perform a job – whether or not that information is inappropriately shared – is a violation of this policy. Every employee, by signing the Confidentiality Agreement agrees not to disclose confidential or proprietary patient care and /or business information to outsiders (including family or friends) or to other employees who do not have a need-to-know.
- 2. Information Disclosure.** Each employee agrees not to discuss confidential patient, employee, payroll, fiscal, research or administrative information where others can overhear the conversation, e.g., in hallways, on elevators, in the cafeterias, on the shuttle buses, on public transportation, at restaurants and at social events. It is not acceptable to discuss clinical information in public areas even if a patient's name is not used. This can raise doubts with patients and visitors about our respect for their privacy.
- 3. Inquiries for Others.** Each employee agrees not to make inquiries for other personnel who do not have proper authority.
- 4. Password Usage.** Each employee is told that they are responsible for information that is accessed with their password. They are responsible for every action that is made while using that password. Thus, they agree not to willingly inform another person of their computer password or knowingly use another person's computer password instead of their own.
- 5. Unauthorized Transmissions.** Employees agree not to make any unauthorized transmissions, inquiries, modifications, or purgings of data in the system. Such unauthorized transmissions include, but are not limited to, removing and/or transferring data from Partner's computer systems to unauthorized locations, e.g., home.
- 6. Responsibilities for Logging Off.** Employees are taught to log off a Partners workstation prior to leaving it unattended. They know that if they do not log off a computer and someone else accessed confidential information while the computer is logged on with their password, they are responsible for the information that is accessed.

Regarding Verbal Communication...

- Patient information should not be discussed where others can overhear the conversation, e.g., in hallways, on elevators, in the cafeterias, on the shuttle buses, on public transportation, at restaurants, or at social events. It is not OK to discuss clinical information in public areas even if a patient's name is not used. This can raise doubts with patients and visitors about our respect for their privacy.
- Dictation of patient information should occur in locations where others cannot overhear.

Regarding Written Information...

- Confidential papers, reports, and computer printouts should be kept in a secure place.
- Confidential papers should be picked up as soon as possible from copiers, mailboxes, conference room tables, and other publicly accessible locations.
- Confidential paper should be appropriately disposed of, e.g., torn or shredded, when they are no longer needed.

Regarding Employee Conduct...

- Employees with access to information about patients, employees, or business matters may only obtain information that is necessary for job performance. *Regardless of the format in which information is obtained, i.e., verbal, written, electronic or other technologic formats yet to be developed, it must be treated with the same level of confidentiality.*
- Accessing any information other than what is required to do your job is a violation of the Partners Confidentiality Policy, *even if you don't tell anyone else.*
- Accessing data must not occur simply to satisfy a curiosity. It is unacceptable to look up data, e.g., a friend's birthday, address or phone number. Information is only viewed when required for one's job.

Regarding Reproducing Patient Information (e.g., faxing, photocopying)...

- Fax machines are the least controllable technology when one transmits patient information. It is critically important when faxing information that the sender has the correct fax number, that they know the receiving fax machine is in a secure location, and that **the patient has signed a Release of Information that allows us to release their health information to another location.**
- Fax Cover sheets should contain the following wording:
"The documents accompanying this fax transmission contain confidential patient information belonging to the sender that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this patient information is prohibited from disclosing the information to any other party. If you have received this transmission in error, please notify that sender immediately and destroy the information that was faxed in error."
- When receiving faxed patient information:
 1. Immediately remove the fax transmission from the fax machine and deliver it to the recipient.
 2. Manage patient information received via fax as confidential in accordance with policy.
 3. Destroy patient information faxed in error and immediately inform the sender.
- The following types of medical information are protected by federal and/or state statute and may NOT be faxed or photocopied outside the individual organization, and/or practice without specific written patient authorization.
Confidential details of:
 1. Psychotherapy (from records of my treatment by a psychiatrist, licensed psychologist or psychiatric clinical nurse specialist)
 2. Other professional services of a licensed psychologist
 3. Social work Counseling/ Therapy
 4. Domestic Violence Victims' Counseling
 5. Sexual Assault Counseling
 6. HIV test results (Patient authorization required for EACH release request)
 7. Records pertaining to Sexually Transmitted Diseases
 8. Alcohol and Drug Abuse Records that are protected by Federal Confidentiality Rules (42 CFR Part 2)
- Questions about faxing patient information, or routine patient information requests should be sent to the Health Information Department.

Regarding Computer Information...

- Sharing a password instead of having your own is prohibited.
- Passwords must not be written down where others can find and/or use them.
- Employees must not log on and let someone else use a computer under their password.
- Employees should protect their data and computer against unauthorized use by:
 - Using virus protection software
 - Locking up backup diskettes or keeping them securely offsite.
 - Locking offices whenever possible.
- Employees must log off the computer system when leaving a workstation.