BRIGHAM AND WOMEN’S HOSPITAL
HUMAN RESOURCES POLICIES AND PROCEDURES

SUBJECT: BREACH OF CONFIDENTIALITY- SANCTIONS FOR
EMPLOYEES AND MEDICAL STAFF
POLICY #: HR-501

EFFECTIVE DATE: February 4, 2012

DEFINITIONS

Confidential Information (CI): Includes Protected Health Information (PHI), personal information (PI), intellectual property, employee information, and any other non-public information that would subject Partners, one who holds or controls access to data, or an individual about whom data is stored, to harm or liability if the data were lost, stolen, accessed, or acquired by unauthorized individuals.

Personal Information (PI): A MA Resident’s first and last name in combination with any one or more of the following:
1. Social Security Number
2. Drivers License Number or state issued ID Number
3. Financial, credit or debit account number that allows a person access to the MA Resident’s financial accounts (i.e. health insurance number)

Note: Personal Information does not include information that is lawfully obtained from publicly available information sources.

POLICY STATEMENT

All suspected breaches of confidentiality and information security will be investigated in conformance with established entity procedures for complaints related to breach of privacy and information security. Sanctions will be applied in accordance with Human Resources policies and/or Medical Staff Bylaws, Rules and Regulations.

BACKGROUND

Access, use and disclosure of any Confidential Information (“CI”) by any employee of Partners HealthCare entities or our affiliated providers must be in accordance with applicable federal and state laws and regulations, including the Privacy and Security Standards associated with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sections 164.530 and 164.308 respectively.
Employees and medical staff are provided training on appropriate procedures related to privacy, security and confidentiality, and are required to abide by the provisions of the policy as summarized and agreed to in the Confidentiality Agreement (Attachment A). Breaches of confidentiality are grounds for disciplinary action up to and including termination of employment or suspension of privileges. Additionally, there are federal (HIPAA) and state laws pertaining to Confidential Information that could result in civil fines, penalties, and/or criminal sanctions against employees or medical staff members; or could result in individual civil lawsuits and judgments.

CATEGORIES OF BREACHES

As a general guideline to managers and medical staff leadership, the following differentiations are made to serve as an aid in the reporting, investigatory and/or disciplinary processes. Additional information/recommendations for type of sanctions that may be applied to each of these categories may be found in Attachment B.

1. **Failing (without purposeful disregard) to demonstrate appropriate care** in handling confidential information in any form or medium (including but not limited to paper, verbal and electronic) that results in accidental access or disclosure, incidental access, or inappropriate access of Confidential Information due to lack of awareness and/or education. Examples include but are not limited to:
   - Failing to sign off a computer terminal when leaving the work area
   - Leaving Confidential Information displayed on computer screens, desks, or work stations where others can view it

2. **Disregard of organization policy** related to the appropriate use and disclosure of Confidential Information, information security policies, or continued demonstration of behaviors listed above. Examples include but are not limited to:
   - Failure to follow appropriate policies with regard to safeguarding Confidential Information that results in potential disclosure of information outside of the organization
   - Leaving Confidential Information unattended in a non-secure area public area or disclosing patient identifiable information by careless telephone use, or discussions in hallways, elevators, the Cafeteria, or other work areas
   - Sharing ID/passwords with co-workers or encouraging them to share
   - Using aggregate data without institutional approval
   - Repeated failure to follow “PH-145: Electronic Communications: Safeguarding PHI.
   - Disabling computer security safeguards such as antivirus software
   - Installing a wireless access router on the Partners network that has not been approved by Partners Information Services

3. **Unauthorized access to, or disclosure of Confidential Information** or repeated violations of previous breaches. Examples include but are not limited to:
   - Accessing Confidential Information on a patient for whom you have no job-related responsibility, including friends and family members
   - Providing ID or password to unauthorized individuals
   - Failure to encrypt a laptop that is used to conduct Partners business or is used to access Partners network resources
4. **Purposeful disregard of organization policies** or repeated demonstrations of behaviors listed above. Examples include but are not limited to:

- Using another employee’s password without their knowledge
- Releasing data for personal gain
- Intentionally using and disclosing Confidential Information requiring patient’s authorization without it
- Destroying or altering Confidential Information intentionally
- Releasing Confidential Information with intent to harm the reputation of an individual or the organization

**ATTACHMENTS:**

Confidentiality Agreement (Attachment A)
Categories of Breaches and Suggested Types of Sanctions (Attachment B)
PARTNERS HEALTHCARE SYSTEM

CONFIDENTIALITY AGREEMENT

Partners HealthCare System, its affiliates and joint venturers, have a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information. Additionally, Partners HealthCare System, its affiliates and joint venturers must assure the confidentiality of its patient, fiscal, research, computer systems, management and other business information. In the course of my employment/assignment at a Partners organization/practice, I may come into the possession of confidential information. In addition, my personal access code [User ID and Password] used to access computer systems is also an integral aspect of this confidential information.

By signing this document I understand the following:

1. Access to confidential information without a patient care/business need-to-know in order to perform my job - whether or not that information is inappropriately shared - is a violation of this policy. I agree 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. I agree not to discuss confidential patient, fiscal, research, computer systems, management and other business 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, 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. I agree not to make inquiries for other personnel who do not have proper authority.

4. I know that I am responsible for information that is accessed with my password. I am responsible for every action that is made while using that password. Thus, I agree not to willingly inform another person of my computer password or knowingly use another person's computer password instead of my own.

5. I 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. I agree to log off a Partners workstation prior to leaving it unattended. I know that if I do not log off a computer and someone else accesses confidential information while the computer is logged on with my password, I am responsible for the information that is accessed.

Partners HealthCare System, its affiliates and joint venturers, and Partners Community HealthCare have the ability to track and monitor access to on-line records and reserves the right to do so. Partners HealthCare System, its affiliates and joint venturers, and Partners Community HealthCare can verify that those who accessed records did so appropriately.

I have read the above special agreement and agree to make only authorized entries for inquiry and changes into the system and to keep all information described above confidential. I understand that violation of this agreement may result in corrective action, up to and including termination of employment and/or suspension and loss of privileges. I understand that in order for any User ID and/or Password to be issued to me, this form must be completed.

____________________
Signature of Employee / Physician / Student / Volunteer / Non-Partners Personnel

_____________________________________________
Date

____________________
Print Name
Human Resources should be notified and is available to assist managers in determining the appropriate sanctions for policy violations. Sanctions will be taken in accordance with Human Resources policies and/or Medical Staff Bylaws, Rules and Regulations. The table below are suggested sanctions meant to provide a guideline in terms of applying reasonable, consistent sanctions in response to each category of breach.

<table>
<thead>
<tr>
<th>Category of Breach</th>
<th>Examples of Breaches</th>
<th>Suggested Sanctions</th>
</tr>
</thead>
</table>
| 1. Failing (without purposeful disregard) to demonstrate appropriate care in handling Confidential Information in any form or medium (including but not limited to paper, verbal, and electronic) that results in accidental access or disclosure, incidental access, or inappropriate access of Confidential Information due to lack of awareness and/or education. | • Failing to sign off a computer terminal when leaving the work area  
• Leaving Confidential Information displayed on computer screens, desks, or work stations where others can view it | • For a first offense depending on the facts, education, a verbal or written warning.  
• For a second offense depending on the facts, education, a written warning or a final written warning.  
• Subsequent offenses depending on the facts, termination. |
| 2. Disregard of organization policy related to the appropriate use and disclosure of Confidential Information, information security policies, or continued demonstration of behaviors listed above. | • Failure to follow appropriate policies with regard to safeguarding Confidential Information that results in potential disclosure of information outside of the organization  
• Leaving Confidential Information unattended in a non-secure area, public area or disclosing patient identifiable information by careless telephone use, or discussions in hallways, elevators, the Cafeteria, or other work areas  
• Sharing ID/passwords with co-workers or encouraging them to share  
• Using aggregate data without institutional approval  
• Repeated failure to follow “PH-145: Electronic Communications: Safeguarding PHI.”  
• Disabling computer security safeguards such as antivirus software  
• Installing a wireless access router on the Partners network that has not been approved by Partners Information Services | • For a first offense depending on the facts, a written or final written warning with education.  
• Subsequent offenses depending on the facts, a final written warning or termination. Except in the case of termination, the employee is required to attend training as soon as possible. |
| 3. Unauthorized access to, or disclosure of Confidential Information or repeated violations | • Accessing Confidential Information on a patient for whom you have no job-related | • For a first offense depending on the facts, a final written warning or |
| 4. Purposeful disregard of organization policies or repeated demonstrations of behaviors listed above. | - Using another employee’s password without their knowledge  
- Releasing data for personal gain  
- Intentionally using and disclosing Confidential Information requiring patient’s authorization without it  
- Destroying or altering Confidential Information intentionally  
- Releasing Confidential Information with intent to harm the reputation of an individual or the organization | - For a first offense depending on the facts, a final written warning, but most likely termination. The employee is required to attend training before returning to work.  
- For a second offense depending on the facts, termination. |