6.11 Describe policies and procedures for ensuring protection of confidentiality, privacy and security for patients and staff and monitoring systems for ensuring compliance.

Concern for patient and staff privacy, confidentiality and security is reflected throughout the organization. There are multiple approaches to maintaining patient and staff confidentiality and to protect the security of all those who enter the hospital environment. These efforts are evident throughout the hospital’s policies, in employee training programs and the hospital’s monitoring systems to ensure compliance, as described in Force 14.5.

Confidentiality and Security Policies

Massachusetts General Hospital (MGH) policies address both patient and employee privacy, security and confidentiality rights. The policies are specific and use language that is unequivocal in emphasizing the importance of confidentiality and privacy. They address expectations around employee actions and compliance with monitoring and regulatory requirements to safeguard patient and employee confidentiality. Numerous policies are also in place to ensure the safety of patients and security of employees. These issues are addressed in policies in the Privacy and Security Manual, the Clinical Policy and Procedure Manual, the Administrative policies and procedures and the Human Resource Policy and Procedure Manual.

The Table of Confidentiality, Privacy and Security Resources (attachment 6.11.a) outlines the full set of policies and resources designed to ensure the protection of confidentiality, privacy and security for employees and patients. Following is a brief description of a portion of the policies in these manuals to illustrate the clear expectations regarding patient and employee confidentiality. Policies not included as an attachment with this force will be available on-site for review.

- Privacy and Security Manual

  Electronic Communications: Safeguarding Protected Health Information (OOD 17) - This policy sets the standard for confidentiality for all protected health information, whether verbal, paper-based, electronic, or other technologic formats yet to be developed. It includes, but is not limited to the following communication tools: electronic mail (e-mail), telephones, cell phones, facsimiles (fax), pagers, PDAs, laptop computers and the Internet. The policy addresses precautions to minimize risks and to safeguard protected information, guidelines for clinician to clinician and clinician to patient communications and guidelines for password protected devices.
Reporting Privacy and Security Violations – This policy defines the scope of privacy and security violations and describes the reporting procedure and process for investigating a reported complaint.

• Clinical Policy and Procedure Manual

  Patient Record - This policy defines the MGH patient’s health record and the documentation, access, security and audit requirements for all patient record keeping across the MGH continuum of care. One section of the policy addresses the core functions of the health record. It states the health record shall promote:
  ♦ Efficient documentation of all aspects of patient care;
  ♦ Timely and accurate incorporation of paper documents into the electronic record by document scanning or other means;
  ♦ Confidential communication of results from clinician to patient, and communication of patient information among clinicians caring for the same patient;
  ♦ Analysis of data to assess quality of care;
  ♦ Decision support for patient safety;
  ♦ Audit of individuals accessing each patient's electronic record.

Quality Policy on Data Management - This policy on performance improvement (PI) data management is to promote transparency in reporting to support an environment of continuous quality improvement while balancing concerns about individual, and institutional confidentiality. It applies to physicians, nurses, allied health professionals, administrators, and support staff at the MGH and Mass General Physician’s Organization’s (MGPO) All development and dissemination of PI data at the MGH/MGPO should be governed by the “need to know” principle, in other words, those using the data must have a need to know the findings in order to perform the tasks they are authorized to perform.

• Administrative Policy Manual

  Code of Conduct - This policy sets forth the principles of conduct intended to govern the actions of employees. Confidentiality included in this policy speaks to expected employee behavior when performing their jobs as it relates to patient care and business operations and the
hospital’s proprietary information including: business strategies, pricing information, financial data, research protocols and intellectual property of the hospital. Section 5.1 of the Code of Conduct states:

_Individuals are expected to treat confidential information obtained through their employment or service to Partners with the utmost confidentiality. Information learned about a patient’s medical treatment or condition is considered confidential as a matter of law and should be treated with particular care. Various state and federal laws and regulations further protect certain types of information about a patient. It is essential, therefore, that individuals adhere to all applicable laws regarding the confidential and privileged status of medical records and communications. This information should be shared within Partners only as appropriate to ensure optimum patient care and as provided in established policies regarding matters, such as, medical records, quality assurance, risk management, utilization review, administration, human studies and research._

**Information Management: General Principles of Information Security** - This policy states the use and management of information at MGH is guided by these principles: information is a corporate asset and must be protected as such protection of privacy is of utmost importance and that all information relating to patients, staff and MGH business demands stringent safeguards and that all external rules and regulations, as well as internal policies and procedures governing the use of information, must be honored. It further outlines the scope, underlying principles and responsibilities related to information security.

**Patient Condition Reporting** - This policy serves as a guide for staff in reporting patient information to any outside inquiry and the media. It states that all patients have the option of stating that they do not want individually identifiable information, including the confirmation of their presence in the facility and/or their condition disclosed.

**Patient Limited Access** - This policy outlines that patients may be placed on either a partial or full limited access list. It is meant to clarify for staff the appropriate response when there is a need to restrict or limit information and access. This policy is often exercised for victims of domestic violence, gang-related individuals, high profile patients and employees.

Confidential Information - (OOD 17) This Human Resource Policy provides the framework for confidentiality and security at MGH. It declares that a wide variety of information is confidential, and that access to confidential data is permitted only when authorized. It also states that employee records and any information learned about a patient, is to be treated as highly confidential. Confidentiality is specifically included in this policy, outlines expected employee behavior when performing their jobs.

Electronic Communication - This Human Resources Policy states personnel shall use electronic communication systems only as authorized by the Hospital and that employees engaging in prohibited activities or violating confidentiality will be subject to corrective action up to and including dismissal. This policy defines electronic communication broadly, specifies prohibited activities, and defines employee responsibilities regarding passwords. The policy explicitly states that employees are expected to use electronic communications in a way that respects the confidential information of others. Staff must use special discretion in transmitting patient identifying information by electronic communication. Transmission must occur in a way that guarantees it will be seen only by a recipient who has a "need to know" the information. In addition, the policy clearly reserves the right of the hospital to review or inspect for legitimate business reasons, the content of any electronic communication vehicle.

Employee ID and Passwords

Employee personnel records are also protected by the structure of the electronic database, which can only be accessed by designated line managers. The hospital also recognizes that many employees are also patients. To keep this distinction, the employee’s identification number and their medical record number are distinct entities to further protect their confidentiality as a patient.

To ensure a greater level of security, in January 2007, the hospital switched to a system whereby computer passwords will expire every 180 days. This policy change requires all MGH employees and professional staff to change their network computer log-on password, twice a year, through a new system called Password Self-Service. This system allows employees to create, change, and manage their own passwords from their computer terminals.
Training and Education

Education is also an important component of ensuring confidentiality and privacy for patients and employees. During hospital orientation, all new employees sign an initial confidentiality statement (attachment 6.11.b) and receive extensive training reviewing HIPAA the guidelines on privacy, security and patient confidentiality.

After orientation, each manager in the hospital is responsible for annual Privacy & Security training within his or her own department. Employees are required to sign a confidentiality agreement stating that they have completed mandatory Privacy & Security Training and reviewed the confidentiality policies during their annual performance appraisal. Managers must submit the signed confidentiality agreement, along with the Performance Evaluation to Human Resources.

All staff in the Department of Nursing reaffirms their confidentiality agreement at the time of their annual performance review. This agreement is imbedded in the performance appraisal tool as evidenced in attachment 6.11.c. These statements are both an educational tool and a method of documenting staffs' review of the confidentiality standards. Additionally, issues of privacy, confidentiality, HIPAA and security are addressed during the Department of Nursing orientation and are elements of the department’s annual training and competency requirements as described in Force 4.18 and Force 14.5.

Monitoring Systems

Monitoring of confidentiality in the institution is multidimensional. The two broad categories of monitoring are proactive monitoring and responsive monitoring:

- Proactive monitoring
  - Guidelines for reporting are in place for employees who suspect and/or are aware of a breach in confidentiality.
  - Partners Information System has a monitoring activity that allows authorized users to determine who has accessed their own record. A Self-Audit function within the Partners computer applications enables all employees who are patients to view a list of users who have accessed their electronic health information. Attachment 6.11.c outlines the procedure for employees.
  - The Health Information Management System has a routine audit of patient medical records in place. A number of charts are reviewed in their entirety each month, evaluating both the paper record and the electronic record. Follow-up, if indicated, is part of the audit process.
- Reactive monitoring
  - A patient or family has the right to request disclosures of their protected health information. Requests are made through the MGH Health Information Services staff.
  - Employees have a mechanism to report breaches in confidentiality as described in the Reporting Privacy and Security Violations policy. Employee reporting is seen as both reactive and proactive.
  - When a suspected breach of confidentiality in relation to patient records has occurred, the incident is investigated in accordance with the guideline “Privacy and Security Violations Subject to Sanctions” (OOD 17).
<table>
<thead>
<tr>
<th>Source</th>
<th>Resource Description</th>
<th>Title of Policy or Resource Tools</th>
</tr>
</thead>
</table>
|        | Policies addressing confidentiality, privacy and security issues for patients and employees | - Abandoned Newborn: Safe Haven*  
- Access Control*  
- Bomb Threats*  
- Code of Conduct  
- Disaster Response Plans and Systems*  
- Firearms*  
- Information Management: General Principles of Information Security; MGH Network Security: Inter-Network Security; Electronic Mail; Data Export  
- Patient Condition Reporting  
- Patient Limited Access  
- Safety Escorts*  
- Threats and Harassment* |
| Online Administrative Manual | Serves as a guide to help maintain an inclusive workplace environment where all members of the work force feel welcomed, respected and supported regardless of any individual differences. | - Confidential Information  
- Recruitment, New Hire and Termination*  
- Electronic Communication  
- Sexual Harassment*  
- Violence and/or threats of Violence* |
| Online Human Resources Policy and Procedure Manual | Policies addressing clinical practice issues and the care of patients | - Neglect or Abuse Policies*  
- Domestic Violence*  
- End of Life Care*  
- Informed Consent*  
- Law Enforcement Personnel: Patient Supervision*  
- On Site Review by Nurses from Outside Agencies*  
- Patient Record  
- Patient Rights Notification*  
- Quality Policy on Data Management |
<table>
<thead>
<tr>
<th>Source</th>
<th>Resource Description</th>
<th>Title of Policy or Resource Tools</th>
</tr>
</thead>
</table>
| Online Privacy and Security Manual         | Policies for employees related the hospital’s health information systems protecting patient and employee information in accordance to HIPAA regulations                                                                                       | ▪ Access (for MGH employees) to Clinical Information Systems  
▪ Accounting of Disclosures of Protected Health Information*  
▪ Auditing and Monitoring Access to Protected Health Information*  
▪ Electronic Communications: Safeguarding Protected Health Information  
▪ Obtaining Authorization for Release of Protected or Privileged Health Information*  
▪ Privacy and Security Violations Subject to Sanctions*  
▪ Reporting Privacy and Security Violations  
▪ Use and Disclosure of Protected Health Information*  
▪ Training Resources: New Orientation, General Privacy & Security, training in Spanish and Haitian Creole  
▪ Manager’s Privacy and Security Training Tool Kit  
▪ Safe Practices Tip Sheets  
▪ Resource Information Guide  
▪ 2006 - 2007 Annual Assessment of Competency |
| HIPAA Resource Intranet Website            | Centralized hospital-wide resource for HIPAA information including: training materials, policies and procedures                                                                                                                                  | ▪ New Hire Education  
▪ Dept. of Nursing Orientation  
▪ Annual Performance Competence Agreement  
▪ 2006 - 2007 Annual Assessment of Competency |
| Patient Care Services                      | Training and education programs for nursing staff                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                 |

*Policies not provided in Overview Documents will be available on-site*
PARTNERS HEALTHCARE SYSTEM, INC.
PARTNERS COMMUNITY HEALTHCARE, INC.
CONFIDENTIALITY AGREEMENT (Orientation)

Partners HealthCare System, its affiliates, and Partners Community HealthCare 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 Partners Community HealthCare must assure the confidentiality of its human resources, payroll, fiscal, research, computer systems, and management 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(s)” and PASSWORD(s)] used to access computer systems is also an integral aspect of this confidential information.

By signing this document I understand the following:

1. I agree not to disclose or discuss any patient, human resources, payroll, fiscal, research and/or management information with others, including friends or family, who do not have a need-to-know.
2. I agree not to access any information, or utilize equipment, other than what is required to do my job, even if I don’t tell anyone else.
3. I agree not to discuss patient, human resources, 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, 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.
4. I agree not to make inquiries for other personnel who do not have proper authority.
5. I agree not to willingly inform another person of my computer password or knowingly use another person’s computer password instead of my own for any reason.
6. 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.
7. I agree to log off prior to leaving any computer or terminal unattended.

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. I further understand that computer access activity is subject to audit.

Please indicate the institution(s) with which you are affiliated:

- Brigham and Women's Hospital
- Dana-Farber Cancer Institute
- Massachusetts General Hospital
- McLean Hospital
- North Shore Medical Center
- Partners HealthCare System
- Partners Community HealthCare
- Spaulding Rehabilitation Hospital
- Other: ____________________________

______________________________
Signature of Employee / Physician / Student / Volunteer

______________________________
Print Name
HOW TO USE THE SELF-AUDIT FUNCTION

OVERVIEW
Partners HealthCare is implementing a Self-Audit function within the Partners computer applications. This application allows employees who are patients of MGH or BWH, to view a list of users who have accessed their electronic health information. Any employee, particularly those without computer self audit access, can manually request an audit through the Privacy Office in Health Information Services or the Office of Patient Advocacy. The Self-Audit Function is available on any Partners workstation.

INSTRUCTIONS FOR USING THE SELF-AUDIT
To access the Self-Audit Function, do the following:
♦ Click on the Start button
♦ Click on Partners Applications
♦ Click on Utilities
♦ Click on Self-Audit
♦ The Self-Audit data are stored for the previous 12 months. There is a drop down button where a selection can be made. Select the desired time range and click “Get Audit Data” to obtain your audit information.
♦ The Current Job Title or Department links the employee’s name to their current job (which may or may not be the same as the job the person had when the access occurred).
♦ The Application column lists the system in which the access occurred, e.g., Clinical Application Suite (CAS), Longitudinal Medical Record (LMR), Brigham Integrated Computer System (BICS)
♦ Any column can be sorted either alphabetically or by date by simply clicking on that column heading.
♦ You can print this report by clicking File on the toolbar and then clicking Print. Be very careful if you print your Audit report. Leaving it lying on a desk or table might leave your information available for others to see.
THINGS TO THINK ABOUT OR KNOW AS YOU REVIEW YOUR SELF-AUDIT REPORT

1. There are many people who need to look at your health information in order to do their job, e.g., registration staff, billing staff. Access to clinical information is not just limited to your doctor or nurse. Most of the names on your report will probably be unfamiliar to you. As you look at the report think about any episodes of care in the past that you had. Could the departments or people on the report link to that episode of care (or the billing for that episode)?

2. The audit report lists the department in which the person is listed at the time you run the audit report. It’s possible that a person listed on your audit report could now be working in a different department than they were when they accessed your record.

3. You may or may not see your physician’s name on the audit report. If you don’t see it, do not assume that he or she has not seen or reviewed your health information, e.g., lab results, x-ray results. Physicians and nurses often have reports/results sent directly to them, or they refer to your paper medical record directly.

If You Suspect that an Unauthorized Access of Your Health Information Has Occurred

1. First and foremost, do not contact the employee yourself.

2. If you suspect that an unauthorized access to their record has occurred, please contact one of the followings:
   - Health Information Services Privacy Office
   - Office of Patient Advocacy/Relations
   - Your manager

3. One of the above-mentioned people will look at your Self-Audit report with you. Then, they will review the accesses with the manager of the employee who you think has breached your confidentiality in order to determine the appropriateness of access and whether or not the employee in question had a “need-to-know” the health information in order to perform his or her duties. If necessary, additional departments may assist in the investigation of the access, e.g., Human Resources, Police and Security.

4. If inappropriate access is determined to have occurred, disciplinary action, up to and including termination of employment or loss of privileges, will be taken.

Reminders About Confidentiality

1. It is a breach of confidentiality to access an employee’s demographic information, e.g., address, phone number, unless you are doing so as part of your job.

2. Sharing a password instead of having your own password is prohibited.

3. Passwords must not be written down where others can find and/or use them.

4. Employees must not log on and let someone else use a computer under their password.
5. You should always log off your computer when you are done. If you do not log off, someone else can look up patient or employee’s health information and it will appear as if you looked it up yourself. If that happens, you will be considered to have breached confidentiality.

6. Managers must notify the appropriate individuals in IS to have computer access changed or turned off when an employee not in the PeopleSoft System changes or leaves their position.

Remember…it is your responsibility to keep patient and hospital information whether it is spoken, written, in a computer system, or just in your head –totally confidential.