Privacy and Security Awareness Training – (Revised 07/2014)
For all Emory Healthcare Workforce Members, Temporary Employees, Contractors, Vendors, Students, and Emory University employees

The Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules regulate the use, disclosure, privacy, confidentiality and security of Protected Health Information (PHI) in written, verbal and the transmission, storage and disposal of PHI in electronic form.

In this document you will learn:
- To identify PHI and patient information to be protected
- To better understand how to protect PHI and the risks when using and storing PHI & ePHI.
- To better understand how to reduce those risks

What are we going to cover?
- Patient Health Information (PHI) and Electronic Patient Health Information (ePHI)
- Privacy & Security Reminders
- Protection from Malicious Software
- Log-In Monitoring
- Password Management
- Sanctions

Standards for Privacy of Individually Identifiable Health Information (IIHI)
- To protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information.
- To improve the quality of health care in the United States by restoring the trust in the health care systems among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care.
- To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems and individual organizations and individuals.

Definition of Privacy
- The right of an individual to be left alone, including freedom from intrusion into one’s private affairs and the right to maintain control over certain personal information.

Definition of Confidentiality
- The responsibility for limiting disclosure of private matters including the responsibility to use, disclose, or release such information with the knowledge and consent of the individual.

Definition of Security
- The means to control access and protect information from accidental or intentional disclosure to unauthorized personnel and from alteration, destruction or loss.
Definition of PHI

- Protected Health Information (PHI)
  - Is any health information that may identify the patient and that relates to:
    - Past, present or future physical or mental health condition; or
    - Healthcare services provided; or
    - Payment for healthcare
    - Includes all communication media – written, electronic and verbal.
    - Extends to all individually identifiable health information in the hands of Emory Healthcare.

- Identifiers of Protected PHI

  - Name
  - Address
  - Zip
  - Names of relatives
  - Name of employer
  - DOB
  - Telephone number
  - Fax number
  - E-mail address
  - Finger or voice prints
  - Photographic images
  - SSN
  - Medical record number
  - Health plan beneficiary number
  - Account number
  - Certificate/license number
  - Vehicle or other device serial number
  - IP address any other unique identifier, character, code

(Any other identifying information that could reasonably identify the patient)

- Examples
  - Financial records
  - Test results
  - Data stored on Intranet/Internet
  - Data used for research purposes
  - A patient’s identification bracelet
  - Medical record number and diagnosis

De-Identification of PHI and Limited Data Sets

Definition of De-Identification

- Health information that does not identify an individual and that there is no reasonable basis to believe that the information can identify an individual is not individually identifiable health information.
  - Health information is considered de-identified if:
    - It has been determined by the appropriate person that the risk is very small that the information could be used to identify an individual.
    - It meets the safe harbor method which is the removal of all of the individual identifiers from the health information.
    - EHC may de-identify information and use codes or other similar means of marking records so they may be later re-identified.

What is Electronic Patient Health Information (ePHI)?

- The definition of ePHI includes any PHI created, received, stored on hard drives, networks laptops, memory sticks and PDAs; contained in e-mail; or transmitted electronically.
Examples of ePHI include, but are not limited to:
- Laboratory results that are emailed to a patient,
- Demographic information about a patient contained in EHC information systems such as Power Chart and Millennium
- A note regarding a patient stored on your Palm Pilot
- Billing Information that is saved to a CD or disk, and
- A digital photograph of a patient stored on your hard drive.

Security

Isn’t this just an Information Technology Problem? NO ! ! ! !

Good security Standards follow the “90/10” Rule:
- 10% of security safeguards are technical
- 90% of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices
  - Example: The lock on the door is the 10%. You remembering to lock the door, check to see if it is closed, ensuring others do not prop the door open, and keeping control of your keys is the 90%.

Risks

- What do I need to do to protect ePHI, PHI or other confidential information?
  - at my EHC workstation
  - on a mobile device

- First: Understand the Risks:
  - Identify the risks at your workstation or in your area of work, for example
    - Shared passwords
    - Failure to log off after each use
    - Use of unlicensed software
    - Viruses
    - Unlocked offices and file cabinets
    - Medical Records laying on a nursing station
    - WOW Carts not disconnected
  - Reduce risks at your workstations and in your work area
  - Get help with Questions or Concerns
  - Report suspected Security and Privacy incidents/breaches

Security Reminders

** Be ALERT to Reminders and follow directions accordingly **

- What are Security Reminders?
  - Ensure that periodic security updates are issued to the workforce concerning EHC policies and procedures
  - Warnings are issued to the workforce of potential, discovered or reported threats, breaches, vulnerabilities or other HIPAA security incidents
  - EHC Information Services Security Policies
  - Security Messages on Logon banners
  - Security Best Practices (i.e., how to choose a good password, how to report a security incident)
  - They can be sent via email “IS Announcements”
Protection from Malicious Software:

Emory Healthcare has developed and implemented procedures for guarding against, detecting and reporting new and potential threats from malicious code such as viruses, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents and procedures.

- **NEVER** open an email attachment, unless you know who sent it and why.
  - If in doubt, call the sender of the email to confirm that the attachment is safe and valid
- **ALWAYS** run an updated Antivirus tool, Do NOT cancel the scheduled scan
- **NEVER** load software that you or your Department is not licensed to use on an EHC workstation.
- **ALWAYS** close “pop-ups” when they solicit a response to advertisements or other messages
  - Click the “x” box to close the pop-up ads
  - Clicking “No” is the same as clicking “Yes” and allows the virus or hacker access to your workstation

Email

* Be AWARE Email is Never 100% secure. **

- Do NOT forward humor stories, chain letters, political or religious views, e-cards, etc.
- **NEVER** send, reply or forward Emory ePHI to a non-Emory mail account (IE: Yahoo, Hotmail, AOL, or gmail etc.)
- Be vigilant when e-mailing patients.
- Don’t forget an e-mail address is a patient identifier.

** When using the Emory/Emory Healthcare MS Exchange email system, please ensure you are sending emails securely to an approved user, by following these steps:
1. All emails sent to an Emory healthcare (@emoryhealthcare.org) email address are SECURE!
2. For an Emory University (@emory.edu) email address, you must do the following to ensure it is Secured:
   a. Locate user in Global Address list (GAL) or address book
b. Verify the icon to the left of the user:

1. if it is a little red person: Then the email is secured and it is OK to email this person.

2. If it is little red person with a globe in front: DO NOT send the user any emails containing ePHI or sensitive emails.

Logon and Access Monitoring
- Emory Healthcare monitors your logon attempts to the EHc electronic Information Systems
- You must ONLY access EHc Information Systems through YOUR userid and password.
- If you do NOT share a computer, and you notice another user signed onto your workstation while you were away; either confirm the user had their own logon id or report it to the Call Center immediately.

Incident Handling
- Report erratic workstation behavior or unusual Email messages to your department Manager, Dept. IS resource or EHc Call Center.
- Report any suspected issues or incidents to a manager or the EHc Call Center
- Report lost or stolen devices to EHC IS department and the Emory Police Department and when appropriate to the Local Police.

Passwords
- Protect your userid and password. YOU are responsible for actions taken with you userid and password
  - Do NOT post, write or share passwords with anyone.
  - The HIPAA Security Rule requires EHc to be able to audit an individuals actions using ePHI.
  - Protect you userid and password from fraudulent use or unethical behavior.

- Use STRONG passwords that are hard to guess, easy to remember and change them often.
  - Do NOT use a word from a dictionary - English or otherwise.
  - Create a password of exactly 8 characters (letters or numbers)
  - Or use a pass phrase to help you remember your password; like:
      - EGBDFPTG (every good boy does fine playing the guitar) or
      - ILUV2GLF (I Love to Golf)

- Use password protected Screen savers on EHC workstations, laptops, and PDAs
- Always Logoff/Disconnet from shared workstations.
  - If you do not logoff, someone else could use your userid to illegally access ePHI.

Patients Rights
- Right to receive a notice describing the covered entity's privacy practices.
- Inform patients how to file complaints, either with the covered entity or DHHS.
- Identify a contact person who can provide additional information.
- Right to access, inspect, and copy protected health information that is used, in whole or in part, to make decisions about them.
- Right to request amendment of protected health information.
- Right to receive an accounting of disclosures made by a covered entity for purposes other than treatment, payment, and health care operations made within six years prior to the request.
- The accounting must be provided within 60 days after receipt of the request.
- Right to request restrictions on the use and disclosure of their protected health information.
- Patients may ask health care providers and plans to communicate health information to them by “alternative means” or at “alternative locations”.

Sanctions
- A violation of the Security Rule could also be a violation of the Privacy Rule and State Laws
- Civil Monetary Penalties range from:
  - Where the person did not know, and by exercising reasonable diligence would not have known:
    o $100 for each violation
    o Not to exceed $25,000 in a calendar year
  - Where the violation was due to reasonable cause and not to willful neglect:
    o $1,000 for each violation
    o Not to exceed $100,000 in a calendar year
  - Where the violation was due to willful neglect and was corrected:
    o $10,000 for each violation
    o Not to exceed $250,000 in a calendar year
  - Where the violation was due to willful neglect and was not corrected:
    o $50,000 for each violation
    o Not to exceed $1,500,000 in a calendar year
- Criminal Penalties
  - Range from $50,000 - $250,000 and imprisonment for a term of 1 – 10 years
  - EHe corrective and disciplinary actions, up to and including termination

Revised 7/2014
Acknowledgement of Privacy and Security Awareness Training

For Emory Healthcare Temporary Employees, Contractors, Vendors, Students, and Emory University employees

I am, or in the future may become, a user of one or more Emory Healthcare information technology devices or systems that may include electronic Protected Health Information (ePHI) and Protected Health Information (PHI) in any other medium and I hereby certify that:

1. I have reviewed the Emory Healthcare “Privacy and Security Awareness Training” handout.

2. I recognize the importance of maintaining the confidentiality and integrity of the ePHI and PHI that I work with for my job duties.

3. I agree to abide by the Emory Healthcare policies and procedures as explained in the Emory Healthcare “Privacy and Security Awareness Training” handouts.

4. I understand that, by not following Emory Healthcare policies and procedures, I could be subject to disciplinary actions or civil or criminal penalties.

5. I have had an opportunity to ask questions. I can call 404-778-2757 if I have questions.

SIGNATURE and AFFILIATION

DATE

PRINT NAME

DEPARTMENT/SECTION

FAX this completed form along with the signed Confidentiality Statement to EHC IS Access Management – 404-727-0759
CONFIDENTIALITY STATEMENT—(Revised 7/2014)

It is the policy of Emory University Hospital, Emory University Hospital Midtown, Emory Healthcare, Inc., The Emory Clinic, Inc., Wesley Woods Center of Emory University, Emory Johns Creek Hospital, Emory Saint Joseph’s Hospital, Emory Specialty Associates, Emory Rehabilitation Hospital in Partnership with Select Medical, and Emory Rehabilitation Outpatient Center in Partnership with Select Physical Therapy and any other affiliates or joint venture/operating companies, collectively referred to as Emory, that any patient, financial, employee, payroll and related information is strictly confidential and/or proprietary information.

I understand that, in the course of my work, I may learn information which is confidential under federal and state law or which is considered confidential and/or proprietary by Emory, including but not limited to patient medical information, other information considered personal by patients and their families, financial information, and employee and payroll information. I agree to keep confidential all such information, whether verbal, written or computerized, which I learn in the course of my work at Emory. I will not discuss patient or family information with anyone not immediately concerned with or involved with a particular patient’s care or treatment. I will not discuss patient information or organizational information with anyone who does not have a business need to know. In addition, I will not discuss patient or organizational information in public areas (such as elevators, cafeterias, etc.).

I will not access or attempt to access any information unless the information is relevant to my job and I am clearly authorized to access it. I understand that the logon ID, computer password, time and attendance identification number and other credentials (hereinafter ‘credentials’) assigned to me by Emory are to be used solely by me in connection with my authorized access to information. I understand that use of my credentials by anyone other than me is strictly prohibited. I will not share my credentials with anyone and I will take all necessary steps to protect the confidentiality of my credentials.

I understand that the Emory Healthcare (xxx.xxx@emoryhealthcare.org) and Emory University (xxxx@emory.edu) electronic mail, including e-mail with the Emory electronic medical record is Emory property and subject to organizational review and should be used only for business purposes. I also understand and certify that the use of my electronic or digital signature to authenticate documents is the equivalent of my handwritten signature on the documents.

I understand it is my responsibility to read and to abide by any and all policies and procedures regarding the use and distribution of information owned by Emory currently in effect or which may be implemented or revised from time to time. I understand that information access will be monitored and any violation of Emory’s policies and procedures will be reported to the appropriate individual(s) and may result in disciplinary action against me including termination of employment or other affiliation(s) with Emory, as well as prosecution to the fullest extent of the law.

I understand that upon my separation, termination or non-affiliation with Emory, I must delete any and all confidential and/or proprietary information stored on my personal media devices or in my other e-mail accounts.

I HAVE READ THE ABOVE CONFIDENTIALITY STATEMENT AND I AGREE TO COMPLY FULLY WITH ITS TERMS

______________________________  ______________________
Signature Date
AUTHORIZATION TO RELEASE STUDENT RECORDS

TO: Emory University d/b/a Emory University Hospital, Emory University Orthopedic and Spine Hospital and Emory University Hospital Midtown; Emory Johns Creek Hospital, Wesley Woods Center, The Emory Clinic and Emory Children’s Center in Atlanta, Georgia (individually or collectively “Emory”)

RE: ____________________________________________
(Print Name of Student)

As a condition of my participation in an educational training program and with respect thereto, I hereby waive my privacy rights, including but not limited to, any rights pursuant to the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g(b)(2)(B), and grant my permission and authorize ____________________________________________ (hereinafter referred to as the “Institution”) to release any and all of my educational records and information in its possession, including but not limited to, academic record and health information to Emory. I further authorize the release of any information relative to my medical history, physical and mental condition to Emory for purposes of verifying the information provided by me and determining my ability to perform my assignments in the educational training program. I also grant my permission to and authorize Emory to release the above information to the Institution. The purpose of this release and disclosure is to allow Emory and the Institution to exchange information about my medical history and about my performance in an educational training program.

I further agree that this authorization will be valid throughout my educational training program. I further request that you do not disclose any information to any other person or entity without prior written authority from me to do so, unless disclosure is authorized or required by law. I understand that this authorization shall continue in force until revoked by me by providing written notice to the Institution and Emory, except to the extent of any action(s) that has already been taken in accordance with this “Authorization for Release of Records and Information.”

In order to protect my privacy rights and interests, other than those specifically released above, I may elect to not have a witness to my signature below. However, if there is no witness to my signature below, I hereby waive and forfeit any right I might have to contest this release on the basis that there is no witness to my signature below. Further, a copy or facsimile of this “Authorization for Release of Records and Information” may be accepted in lieu of the original.

By signing this “Authorization for Release of Records and Information,” I hereby indemnify and hold harmless the Institution, its members, agents, servants and employees, and Emory and its members, agents, servants and employees (each of the foregoing being hereinafter referred to individually as the “Indemnified Party”) against all claims, demands, causes of action, actions, judgments or other liability including attorney’s fees (other than liability solely the fault of the Indemnified Party) arising out of or in connection with this “Authorization for Release of Records and Information.”

I have read, or have had read to me, the above statements, and understand them as they apply to me. I hereby certify that I am eighteen (18) years of age or older, suffer under no legal disabilities, and that I have freely and voluntarily signed this “Authorization for Release of Records and Information” as of this the ___ day of __________________________, 201__.

Signature
Name: ____________________________________________
(Please print)

Witness Signature
Name: ____________________________________________
(Please print)
Nursing Student / Faculty Computer Logon ID Request Form – 4-11-12

Complete all items. Print legibly. Incomplete or illegible forms will delay issue of logon ID

Last Name: ________________________________________________
First Name: ________________________________________________
Middle Initial: ______________________________________________

Level: circle current status
Sophomore Junior Senior Faculty RN-BSN NP Graduate

School of Nursing: __________________________________________

Social Security Number: _______ ______ ______ ______
Complete SSN Required. Do not put school ID #.
Foreign born students without an SSN may substitute date of birth.

Anticipated Graduation Date: _________________________________

Clinical Department for this rotation: __________________________

Faculty Name: _____________________________________________

Are you a returning student?

_____ No

_____ Yes If yes what is your logon ID? _______________________

Are you a current Emory Healthcare employee?

_____ No

_____ Yes If yes provide the following information:
Current Logon ID: __________________________________________
EHC Job Title: ______________________________________________
Work Department / Entity: ______________________________________
STUDENT AGREEMENT CONCERNING
EDUCATIONAL TRAINING PROGRAM

In consideration for being permitted to participate in a clinical training experience at Emory University
d/b/a Emory University Hospital, Emory University Orthopedic and Spine Hospital and Emory University
Hospital Midtown; Emory Johns Creek Hospital, Wesley Woods Center, The Emory Clinic and Emory
Children’s Center at Emory University in Atlanta, Georgia (individually or collectively referred to herein
as Emory”), I hereby agree to the following:

1. To follow the administrative policies, standards and practices of Emory including, but not limited
to the following:
   a. Students may administer medications when under the direct supervision of Institution’s
      faculty. Direct supervision is defined as retrieving medications from the medication
      room through administration of medications at the bedside. This means that 100% of the
      medication administration process is observed by the Institution’s faculty for every
      medication administered by a student. If for any reason the Institution’s faculty is
      unavailable to supervise the process from the medication room to the patient’s bedside,
      and the medication cannot wait until the Institution’s faculty is available, the patient’s
      nurse will administer the medication.
   b. Two licensed RNs will perform the “double-check” for any medications or procedures
      requiring a “double-check” pursuant to Emory policies and procedures.

2. To report to Emory on time and to follow all established rules and regulations of Emory.

3. To comply with federal and state laws, including but limited to the Health Insurance Portability
   and Accountability Act of 1996 and its accompanying federal regulations, and the rules and
   regulations of Emory regarding the confidentiality of all medical, health, financial and social
   information (including mental health) pertaining to particular clients or patients.

4. To not publish any material related to my educational training program that identifies or uses the
   name of Emory or its members, clients, students, faculty or staff, directly or indirectly, unless I
   have received written permission from Emory.

5. To comply with all federal, state and local laws regarding the use, possession, manufacture or
   distribution of alcohol and controlled substances.

6. To follow Center for Disease Control and Prevention (C.D.C.) Universal Precautions for Blood
   Borne Pathogens, C.D.C. Guidelines for Tuberculosis Infection Control, and Occupational Safety
   and Health Administration (O.S.H.A.) Respiratory Protection Standard.

7. To arrange for and be solely responsible for my living accommodations while at Emory.

8. To provide the necessary and appropriate uniforms and supplies required where not provided by
   Emory.

9. To wear a nametag that clearly identifies me as a student.

I understand and agree that Emory shall not be responsible for any loss, injury or other damage to myself
or my property arising during my participation in the educational training program.

Further, I understand and agree that I will not receive any monetary compensation from Emory for any
services I provide to Emory or its clients, patients or staff as a part of my educational training program.

I also understand and agree that I shall not be deemed to be employed by or an agent or a servant of
Emory; that Emory assumes no responsibilities as to me as may be imposed upon an employer under any
law, regulation or ordinance; and that I am not entitled to any benefits available to employees. Therefore,
I agree not to in any way hold myself out as an employee of Emory.
I understand and agree that I may be immediately withdrawn from the educational training program by Emory based upon a perceived lack of competency on my part, my failure to comply with the rules and policies of Emory, if I pose a direct threat to the health or safety of others or, for any other reason Emory reasonably believes that it is not in the best interest of Emory or Emory’s patients or clients for me to continue.

I understand and agree to show proof of professional liability insurance in amounts satisfactory to Emory, and covering my activities at Emory, and to provide evidence of such insurance upon request of Emory.

I further understand that all medical or health care (emergency or otherwise) that I receive at Emory will be my sole responsibility and expense.

I have read, or have had read to me, the above statements, and understand them as they apply to me. I hereby certify that I am eighteen (18) years of age or older, suffer under no legal disabilities, and that I have freely and voluntarily signed this “Educational Training Program Agreement.”

This the ___ day of ______________________, 201__.

_________________________________________  __________________________________
Signature                                      Witness Signature

Name:__________________________  Name:__________________________
(Please print)                               (Please print)