



Acknowledgement of HIPAA 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). I hereby certify that:

1. I have reviewed the Emory Healthcare “HIPAA Security Awareness Training” handout.
2. I recognize the importance of maintaining the confidentiality and integrity of the ePHI 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 “HIPAA 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.

EMPLOYEE’S SIGNATURE

DATE

PRINT NAME

DEPARTMENT

**FAX this completed form along with the signed Confidentiality Statement
To EHC Security – 404-727-0759**



HIPAA Security Awareness Training

For all Emory Healthcare Workforce Members

The HIPAA Security Rule has been in effect since April 20, 2005. This rule regulates the use of Protected Health Information (PHI) in electronic form “ePHI”. It covers the access, transmission, storage and disposal of PHI in electronic form.

In this document you will learn:

- To better understand the risks when using and storing 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)
- Security Reminders
- Protection from Malicious Software
- Log-In Monitoring
- Password Management
- Sanctions

Definition of PHI

- Protected Health Information
 - 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
 - Examples
 - Financial records
 - Test results
 - Data stored on Intranet/Internet
 - Data used for research purposes
 - A patient’s identification bracelet
 - Sign in sheet that includes a patient’s name and reason for visit

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 IT 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 or other confidential information?
 - at my EHC workstation
 - on a mobile device
- First: Understand the Risks:
 - Identify the risks at your workstation, for example
 - Shared passwords
 - Failure to log off after each use
 - Use of unlicensed software
 - Viruses
 - Reduce risks at your workstations
 - Get help with Questions or Concerns
 - Report suspected Security incidents

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 are 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. **

- NEVER send, reply or forward EHC ePHI from a non-EHC mail account (IE; Yahoo, Hotmail, AOL, emory.edu etc.)
- Do NOT forward humor stories, chain letters, political or religious views, e-cards, etc.

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.
 - 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
 - Use at least 6 characters (letters, numbers or symbols)
 - 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/Disconnect from shared workstations
 - If you do not logoff, someone else could use your userid to illegally access a ePHI

Sanctions

- A violation of the Security Rule could also be a violation of the Privacy Rule and State Laws
- Civil Monetary Penalties range from:
 - \$100 - \$25,000 / year
 - More for multiple year violations
- Criminal Penalties
 - Range from \$50,000 - \$250,000 and imprisonment for a term of 1 – 10 years
- EHC corrective and disciplinary actions, up to and including termination



CONFIDENTIALITY STATEMENT

It is the policy of Emory University Hospital, Crawford Long Hospital, Emory Healthcare, Inc. and The Emory Clinic, Inc. ("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 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 myself 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 electronic mail 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 HAVE READ THE ABOVE CONFIDENTIALITY STATEMENT AND I AGREE TO COMPLY FULLY WITH ITS TERMS

Signature

_____/_____/_____
Date