EMORY
HEALTHCARE

CONFIDENTIALITY STATEMENT– (Revised 3/2021)

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 Decatur Hospital, Emory Hillandale Hospital, Emory Long Term Acute Care, 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, vendor, payroll and related information is strictly confidential and/or proprietary information.

I understand that, in the course of my work or affiliation with Emory (collectively work), I may learn information which is confidential or privileged under federal and state law or which is considered sensitive, confidential and/or proprietary by Emory, including but not limited to patient medical information, other information considered personal by patients and their families, employee and payroll information and non-public and proprietary financial, vendor, and third-party information. I agree to keep confidential all such information, whether verbal, written or electronic, which I learn in the course of my work at or affiliation with 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 other confidential or proprietary information with anyone who does not have a legitimate business-related need to know. In addition, I will not discuss patient or other confidential proprietary information in public areas (such as elevators, cafeterias, etc.).

I will not access or attempt to access or use any electronic system or information unless the information is relevant to my job/work 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 and use of electronic systems and 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 unless otherwise permitted by relevant Emory policies. 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 access and use of Emory electronic systems and the access, use and disclosure of information owned by Emory and other confidential information, as such policies are currently in effect or which may be implemented or revised from time to time. I understand that electronic system and information access may 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, which may include but is not limited to loss or limitation of access to electronic systems with patient information, termination of employment or other affiliation(s) with Emory, including loss of clinic and/or hospital privileges, reporting to my employer (if different from Emory) or law enforcement, as well as prosecution to the fullest extent of the law.

I understand that upon my separation, termination of employment or contractor status or other non-affiliation with Emory, I am not allowed to keep or take, or have in my possession or continue or attempt to access or use, any confidential or proprietary information from Emory Healthcare or Emory University. I understand that following my separation, termination of employment or contractor status or other non-affiliation with Emory my obligations with regard to the use and disclosure of patient and employee information will continue indefinitely and that my confidentiality obligations with regard to all other confidential or proprietary information will continue for so long as the information is not generally available to the public without fault by me.

I UNDERSTAND THAT EMORY IS GRANTING ME ACCESS TO CONFIDENTIAL INFORMATION AND INFORMATION SYSTEMS IN CONSIDERATION OF MY PROMISES IN THIS CONFIDENTIALITY STATEMENT, BY SIGNING, I HAVE READ THE CONFIDENTIALITY STATEMENT AND I AGREE TO COMPLY FULLY WITH ITS TERMS

______________________________________ __________/________/________
Signature Date

EMORY
HEALTHCARE

Acknowledgement of Privacy and Security Awareness Training

For Emory Healthcare Employees, Temporary Employees, Contractors, Vendors, Students, Emory University Employees, Physicians, Community Physicians and All Other Users with Access to ePHI/PHI

I am, or in the future may become, a user of one or more Emory Healthcare (EHC) 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 all ePHI and PHI.

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 am subject to disciplinary actions up to and including termination of employment, loss of hospital and clinic privileges, or other affiliations with EHC, loss of access to systems with ePHI, civil action and penalties, and criminal action and penalties.

5. I can call 404-778-2757 if I have questions regarding the training. I have had an opportunity to ask questions regarding the "Privacy and Security Awareness Training

If you are signing this document in the New Applicant System it will automatically be sent to IS Security on your behalf. Otherwise **FAX this completed form along with the signed Confidentiality Statement to EHC IS Access Management – 404-727-0759 or email scanned forms to issecurity_ehc@emoryhealthcare.org.** You may contact your Access Coordinator with questions regarding logon ID access. **DO NOT** FAX THIS form to the EHC Office of Compliance Programs.

______________________________________ __________

SIGNATUREand AFFILIATION **DATE**

____

PRINT NAME

____

DEPARTMENT/SECTION

EMORY
HEALTHCARE

For Emory Healthcare Employees, Temporary Employees, Contractors, Vendors, Students, Emory University Employees, Physicians, and All Other Users with Access to ePHI/PHI

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 (ePHI).

In this document you will learn:

- To identify Protected Health Information (PHI) and electronic PHI
- How to protect PHI and ePHI and the risks when using and storing PHI and electronic Protected Health information (ePHI)
- How to reduce the risks of breach and inappropriate disclosure of PHI and ePHI.

What are we going to cover?

- Patient Health Information (PHI) and Electronic Patient Health Information (ePHI)
- Privacy and Security Reminders
- Protection from Malicious Software
- Log-In Monitoring
- Password Management
- Sanctions

The Standards for Privacy of Individually Identifiable Health Information (IIHI):

- Protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information.

- 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.

- 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.

Privacy is:

- 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.

Confidentiality is:

- 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.

Security is:

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

Protected Health Information (PHI):

- □ Is any individual identifiable 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 <u>all</u> individually identifiable health information in the hands of Emory Healthcare

- □ Individual Identifiers:
    - – Name
    - – Address
    - – Zip
    - – Names of relatives
    - – Name of employer
    - – Date of birth
    - – Telephone number
    - – Fax number
    - – E-mail address
    - – Finger or voice prints
    - – Photographic images
    - – Social Security Number
    - – 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 reasonable identify the patient

- □ Examples of PHI:
    - – Financial records
    - – Test results
    - – Medical record number
    - – Diagnosis
    - - A patient’s identification bracelet
    - - Data stored on intranet/internet
    - - Data used for research purposes

De-Identification of PHI/ePHI and Limited Data Sets

Definition of De-Identification

- ■ Health Information that does not identify an individual and for which there is no reasonable basis to believe that the information can identify an individual.
    - – 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 re-identified.

Electronic Patient Health Information (ePHI)

- ■ ePHI includes any PHI created, received, stored on hard drives, networks, laptops, memory sticks and personal digital assistance(s) 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 a mobile phone or other mobile device
        - – Billing information that is saved to a CD
        - – A photograph of a patient in electronic format (i.e. digital, scanned)

Security
We are all responsible for keeping our patients' information secure.

- ❑ Good security standards follow the "90/10" Rule:
  - 10% of security safeguards are technical
  - 90% of security safeguards rely on the computer user (that's 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 that others do not prop the door open, and keeping control of your keys is the 90%.
- ❑ To increase security on select applications, Emory has implemented Duo Security. This two-factor authentication adds a second layer of security for your protection by requiring two factors to confirm your identity - something you know (your password) and something you have (e.g., app push, text message, or call to your mobile phone or landline). You must enroll in Duo on a computer (not from a smartphone) to access Emory systems from off campus (off the Emory network or Emory WiFi network), as well as for accessing some HR and/or payroll related systems on campus. Learn more at https://duo.emory.edu

Risks
Protect PHI and ePHI at your workstation and mobile devices by:

- ■ Understanding the Risks:
  - ❑ Identify the risks at your workstation or in your area of work, for example:
    - Sharing passwords
    - Failure to log off after each use
    - Use of unlicensed software
    - Viruses
    - Unlocked offices and file cabinets
    - Medical records laying out on desks or at a nursing station
    - Work on Wheels (WOW) carts not disconnected or logged-off
  - ❑ Reduce risks at your workstations and in your work area
  - ❑ Get help with questions or concerns
  - ❑ Report suspected security and privacy incidents/breaches to management

Security Reminders
* Be alert to and follow Security reminders *

- ❑ 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 security incidents
  - EHC Information Services Security Policies
  - Security messages on logon banners
  - Security best practices (e.g. how to choose a good password, how to report a security incident)
  - Messages contained in EHC system e-mails

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. Don't do it!

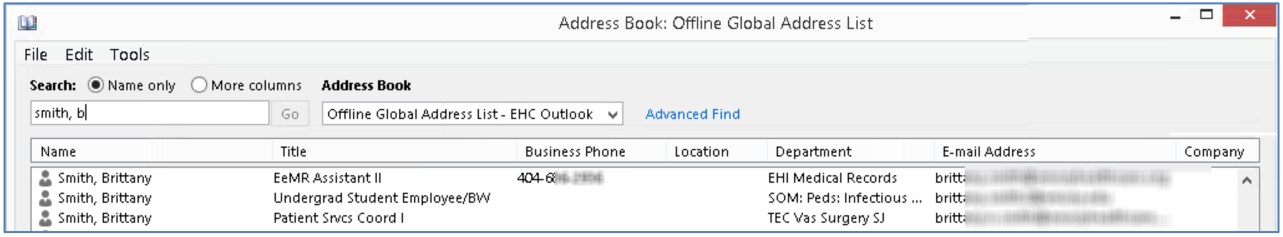
Email

- Be aware that e-mail is never 100% secure. It can be forwarded by the recipient to other persons or printed and left where others can see it.

  - ❑ Encourage patients to utilize the Patient Portal for communication instead of communicating with providers via e-mail.
  - ❑ 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. It is easy to pick the wrong name from the address book without realizing it, so double check your address list before you press send. Use title, department and email address in addition to name to help find the correct person and address.



Address Book: Offline Global Address List

Search: ● Name only ○ More columns

Address Book: Offline Global Address List - EHC Outlook

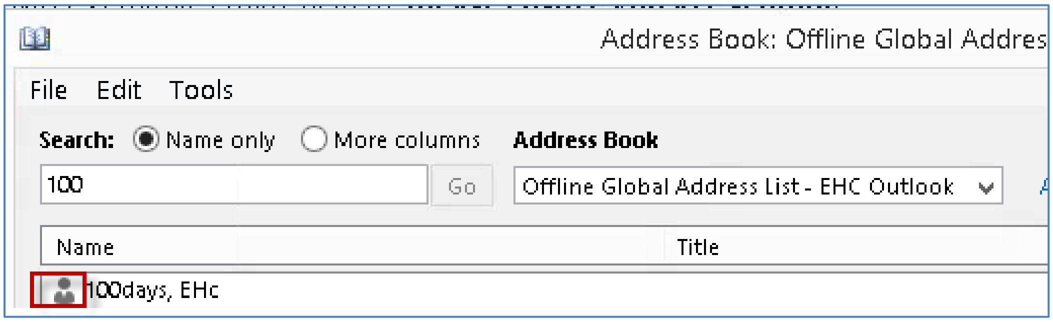
smith, b

Name	Title	Business Phone	Location	Department	E-mail Address	Company
Smith, Brittany	EeMR Assistant II	404-6[redacted]		EHI Medical Records	britt[redacted]	
Smith, Brittany	Undergrad Student Employee/BW			SOM: Peds: Infectious ...	britt[redacted]	
Smith, Brittany	Patient Srvcs Coord I			TEC Vas Surgery SJ	britt[redacted]	

2. All emails sent to an Emory Healthcare (@emoryhealthcare.org) email address are secure!
3. Many physicians and clinical staff have @emory.edu addresses. For an Emory University (@emory.edu) email address, you must do the following to ensure it is secure:
   a. Locate the person in the Global Address list or address book
   b. Verify the icon to the left of the person's name:

      1) If it is a person icon: 👤 then the email is secure and it is OK to email this person.

      2) If it is person in front of a globe: 🌐 **DO NOT send the user any emails containing ePHI or sensitive information**.



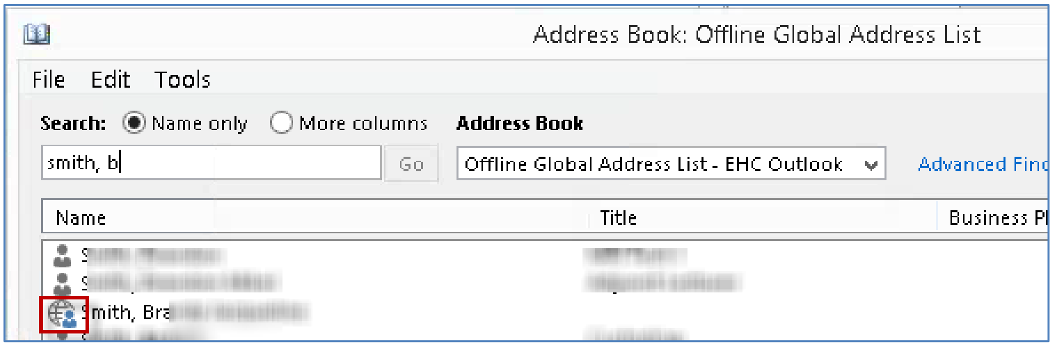
Address Book: Offline Global Addres

Search: ● Name only ○ More columns

Address Book: Offline Global Address List - EHC Outlook

Search: 100

Name	Title
100days, EHc	



Address Book: Offline Global Address List

Search: ● Name only ○ More columns

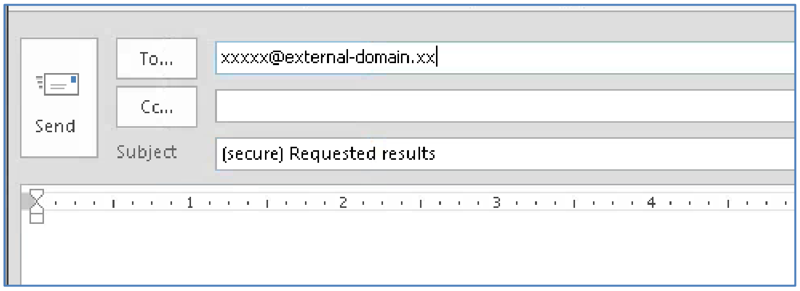
Address Book: Offline Global Address List - EHC Outlook

Search: smith, b

Name	Title	Business Pl
S[redacted]	[redacted]	
S[redacted]	[redacted]	
Smith, Bra[redacted]		

Hint: the globe icon indicates the email address is external to or outside Emory

4. Emory uses Office 365 Message Encryption (OME) to encrypt outgoing email messages. OME allows Emory users to send emails to external users, ensure the message is transmitted securely, and visible only by the intended recipient. To send a secure email to a non-Emory email address (an external email address), you must add either **(encrypt)** OR **(secure)**, including the parentheses, to the subject line of your e-mail message. Do not include ePHI or sensitive information in the Subject line of your message. Adding one of these two tags in the email subject line designates to the email system that this message will be sent encrypted. Compose and send your message as usual.



To... xxxxx@external-domain.xx

Cc...

Subject (secure) Requested results

Information that you can send to the external recipient on how to retrieve the secure message can be found at http://it.emory.edu/office365/ome.html.

- Additional information about email
  - ❑ Use email in support of your job. Do NOT forward humor stories, chain letters, political or religious views, etc.
  - ❑ Email belongs to Emory Healthcare
  - ❑ Email documents can be subpoenaed
  - ❑ Email documents are not “gone” when deleted
  - ❑ **NEVER** click on a web link in an email message and then provide your Logon ID and password and **NEVER** reply to an email message asking for your Logon ID and password.

These are most often phishing attempts. Phishing is an identity theft scheme where someone tries to lure or trick you into revealing your password, credit card number or other confidential information. Don't fall for it!

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 own user ID 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 his/her own logon ID or report it to the EHC Service Desk immediately.

Incident Handling

- Report erratic workstation behavior or unusual e-mail messages to your department Manager, department Information Services resource or EHC Service Desk.
- Report any suspected issues or incidents to a manager or the EHC Service Desk.
- Report lost or stolen devices to EHC Information Services department and the Emory Police Department and, when appropriate, to the local police.

Passwords

- Protect your user-ID and password. You are responsible for actions taken with you user-ID and password.
  - ❑ Do NOT post, write down or share your passwords with anyone.
  - ❑ The HIPAA Security Rule requires EHC to be able to audit an individual's actions using ePHI.
  - ❑ Protect your user-ID 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 between 9 to 30 characters (letters, numbers, and special characters).
  - ❑ Or use a pass phrase and add 2 numbers or a symbol to help you remember your password:
    - – **EGbDF42dY** (every good boy does fine for today) or
    - – **ILV2GLF4fn** (I Love to Golf for fun)

- Use password protected screen savers on EHC workstations, laptops, and cell phones and tablets.
- Always logoff/disconnect from shared workstations.
  - ❑ If you do not logoff, someone else could use your User-ID to illegally access ePHI.

Patient Rights

- Right to receive a notice describing the covered entity's privacy practices.
- Right to file complaint with the Department of Health and Human Services. Inform patients how to file complaints.
- 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 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:
    - $100 for each violation
    - Not to exceed $25,000 in a calendar year
  - Where the violation was due to reasonable cause and not to willful neglect:
    - $1,000 for each violation
    - Not to exceed $100,000 in a calendar year
  - Where the violation was due to willful neglect and was corrected:
    - $10,000 for each violation
    - Not to exceed $250,000 in a calendar year
  - Where the violation was due to willful neglect and was not corrected:
    - $50,000 for each violation
    - 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 to 10 years
- □ EHC corrective and disciplinary actions, up to and including termination