



CONFIDENTIALITY AND SYSTEM ACCESS TERMS– (Revised 7/2022)

In order for Emory Healthcare and its affiliated entities and healthcare facilities (which are individually and collectively referred to as “EHC” in these Terms) to permit authorized users access to certain of EHC’s electronic systems, including but not limited functionality related to EHC’s electronic health records (which are referred to as “EHC Systems” in these Terms), users must agree to be bound by these Confidentiality and System Access Terms (which are referred to as the “Terms”). Users may require access to EHC Systems based on their work for or other affiliation with EHC (which are referred to as the “EHC Affiliation” in these Terms). Examples of EHC Affiliation for which a user requires access to EHC Systems include, but aren’t limited to, working for EHC as an employee, contractor or other service provider, being a medical staff member, and providing treatment or certain other services to current or former EHC patients on behalf of a non-EHC provider or vendor. Users who do not agree to these Terms are not permitted to access or use any EHC Systems.

Certain provisions of these Terms may be superseded by expressly designated legal notices or terms located on particular pages within an EHC System. The Terms may be updated from time to time. The most current version of the Terms will be posted in the [EHC Policy Management System](#). Accordingly, it is the user’s responsibility to periodically review this page to ensure familiarity with the most current version of these Terms. A user’s continued access and use of any EHC System after modifications of the Terms are posted will constitute the user’s agreement to be bound by such updated Terms.

It is the policy of EHC 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 EHC Affiliation, I may learn information which is confidential or privileged under federal or state law or which is considered sensitive, confidential and/or proprietary by EHC (all such information is referred to as “Confidential Information” in these Terms). Depending on the nature of my EHC Affiliation and responsibilities, Confidential Information to which I have access to may include, but is not limited to, patient medical, financial and personal information, employee and payroll information and other non-public and proprietary financial, technical, operational, as well as vendor and other third-party information. I agree to keep confidential all such Confidential Information, whether verbal, written or electronic, which I learn in the course of my EHC Affiliation and to only use or disclose Confidential Information as specifically permitted by EHC for purposes of my specific EHC Affiliation. 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 Information with anyone who does not have a legitimate business-related need to know. In addition, I will not discuss patient or other Confidential Information in public areas (such as elevators, cafeterias, public hallways, etc.).

I will not access or attempt to access or use any EHC System or information unless the information is relevant to my EHC Affiliation and I am clearly authorized to access it. I understand that the logon ID, computer password, time and attendance identification number and other credentials (individually and collectively called the “Credentials” in these Terms) that may be assigned to me by EHC are to be used solely by me in connection with my authorized access to and use of EHC Systems and information. **I understand that use of my Credentials by anyone other than me is strictly prohibited.** I will not share any Credentials with anyone, and I will take all necessary steps to protect the confidentiality of my Credentials.

I understand that the EHC (xxx.xxx@emoryhealthcare.org) and Emory University (xxxx@emory.edu) electronic mail, including messaging within the EHC electronic medical record, is EHC property and subject to organizational review and should be used only for business purposes unless otherwise permitted by relevant EHC policies. I also understand and certify that 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 EHC Systems and the access, use and disclosure of Confidential Information and other information or data owned by EHC, as such policies are currently in effect or which may be implemented or revised from time to time. I understand that EHC Systems and information access may be monitored and violation of EHC's policies and procedures may result in disciplinary action against me, which depending on the nature of my EHC Affiliation may include, but is not limited to, loss or limitation of access to EHC Systems, termination of employment or other affiliation(s) with EHC, including loss of clinic and/or hospital privileges, reporting to my employer (if different from EHC) or law enforcement, as well as civil and criminal prosecution to the fullest extent of the law.

I understand that when my EHC Affiliation ends for any reason, whether because of termination of my employment or contractor status or otherwise, I am not permitted to keep or take, or have in my possession or continue or attempt to access or use, any confidential or proprietary information from EHC or access any EHC Systems, unless specifically authorized by EHC policy. I understand that when my EHC Affiliation ends for any reason 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 Information will continue for so long as the information is not generally available to the public without fault by me.

I UNDERSTAND THAT EHC IS GRANTING ME ACCESS TO CONFIDENTIAL INFORMATION AND EHC SYSTEMS IN CONSIDERATION OF AND RELIANCE ON MY AGREEMENT TO THESE TERMS. BY SIGNING, I ACKNOWLEDGE THAT I HAVE READ AND AGREE TO COMPLY FULLY WITH THESE TERMS.

Signature

_____/_____/_____
Date

INSTRUCTIONS FOR COMPLETING AND RETURNING FORMS:

- If you are accessing and signing these Terms within the EHC New Applicant System, the signed Terms will be automatically sent to EHC following signature.
- If you are requesting Emory Healthcare Link (EpicCare Link) access, you must attach these signed documents to your Emory Healthcare Link access request.
- If you are requesting EpicCare (Epic Hyperspace) access, you must attach these signed documents to your EpicCare access request.
- Otherwise, you must sign and date the Terms, and **email the scanned signed and dated Terms to your access coordinator.**
- You may contact your Access Coordinator with questions regarding logon ID access.
- **DO NOT FAX THIS** form to the EHC Office of Compliance Programs.
- Please note that the completed and signed Acknowledgement of Privacy and Security Awareness Training document must also be received by EHC before access may be granted.



PRIVACY AND SECURITY AWARENESS TRAINING (Revised 07/2022)

Scope:

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 PHI and ePHI
- How to protect PHI and ePHI and the risks when using and storing PHI and ePHI
- How to reduce the risks of breach and inappropriate disclosure of PHI and ePHI

What are we going to cover?

- PHI and 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.

Definitions:

- **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.
- **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.
- **De-Identification of PHI/ePHI and Limited Data Sets:** 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 and documented by an appropriate qualified data expert applying generally accepted statistical and scientific principles and methods 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 if certain regulatory conditions are met.
- **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:

Financial records	Medical information in an e-mail
Test results	Diagnosis
Medical information stored on the intranet/internet	Patient's identification bracelet
A Patient's tattoo if unusual	A Patient's phone number
Medical record number	Laboratory results that are emailed to a patient
Demographic information about a patient contained in EHC information systems such as Epic	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:** 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 all individually identifiable health information in the hands of EHC
- **Individual Identifiable Information:** Health information that is created or received by EHC and relates to the past, present, or future physical or mental health or condition of an individual or payment for the provision of care to the patient, the provision of health care to the patient, and identifies the patient or there is a reasonable basis to believe the information can be used to identify the patient.

Individual Identifiers include, but are not limited to:

Name	Photographic images
Address	Social Security Number
Zip	Medical record number
Names of relatives	Health plan beneficiary number
Name of employer	Account number
Date of birth and all other elements of dates (except year) for dates directly related to an individual, including dates of service	IP address any other unique identifier, character, code
Telephone number	Vehicle or other device serial number
Fax number	Certificate/license number
E-mail address	Any other identifying information that could reasonable identify the patient
Finger or voice prints	

Accessing Patient Information

Users should only access PHI in order to perform their job duties; the type and amount of PHI that they access should be limited to that which is necessary to perform the job duty at hand.

- Do not access the medical records and/or PHI/ePHI of family members, friends, or co-workers through the EHC Electronic Medical Record (EeMR) unless you are actively involved in the patient's care or have been specifically asked to consult in the patient's care by a member of the patient's care team.
- If you are accessing a family member, friend, or co-worker's confidential medical record as a care provider, this role must be documented in the patient's medical record for each stage of care. Inappropriate viewing of these medical records may be grounds for disciplinary action.
- EHC Policy does not permit you to access your own medical record through the EeMR. You may access your own medical record information on the same basis as any other EHC patient. For example, you may access your information through the appropriate Patient Portal or by requesting access from Medical Records/Health Information Management (HIM).
- Do not ask another employee or provider with access to the EeMR or EHC Systems to access your medical record or health information for you as a favor. Doing so may result in disciplinary action against both you and the other employee or provider.

Security

Keeping EHC patients' information private and secure is everyone's responsibility. Users should always report suspected security and privacy incidents/breaches to management.


Passwords

- Protect your user-ID and password
 - **You are responsible for actions taken with you user-ID and password.**
 - The HIPAA Security Rule requires EHC to be able to audit an individual's actions using ePHI
 - Do NOT post, write down or share your passwords with anyone
 - 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 all workstations
- NOTE:** If you do not logoff, someone else could use your User-ID to inappropriately access ePHI.

Logon and Access Monitoring

- You must ONLY access EHC Information Systems through your own user ID and password
- EHC monitors your logons and logon attempts to the EHC electronic Information Systems
- To increase security on select applications, EHC 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 to access some EHC systems from off campus (off the EHC network or EHC Wi-Fi network), as well as for accessing some HR and/or payroll related systems on campus. Learn more at <https://ourehc.org/departments/is/Security/duo/index.html>

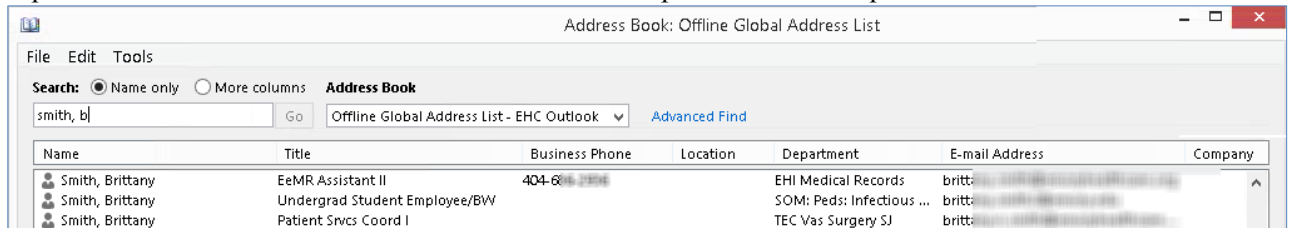
Workspace and Device Security

- Protect your workspace by:
 - Locking your workstation when unattended by pressing Ctrl + Alt + Del and then choose lock workstation, or by pressing the Windows key and L.
- 
- Avoid displaying any sensitive information on screen or monitor in a public area
 - Ensuring unattended offices and file cabinets that store PHI are locked
 - Do NOT leave Medical records laying out on desks or at a nursing station
 - Always securely dispose of printed PHI
- **Physically secure devices:**
 - Never leave any laptop, mobile device or thumb drive containing ePHI in your vehicle Do not store ePHI on non-encrypted mobile devices or thumb drives
- **Protection from Malicious Software:**
 - Do NOT 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.
 - If on an EHC workstation, do NOT load software that you or your department is not licensed to use.
 - 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!
- **Security Reminders and Updates**
 - Be on the lookout for and review security reminders and update sent from EHC. Reminders and updates could include:
 - Periodic security updates that 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 best practices (e.g., how to choose a good password, how to report a security incident)

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.
- **Please ensure you are sending emails securely to an approved user!**
 - Make sure you choose the correct recipient. 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

File Edit Tools

Search: Name only More columns **Address Book**

Name	Title	Business Phone	Location	Department	E-mail Address	Company
Smith, Brittany	EeMR Assistant II	404-688-2296		EHI Medical Records	britt: [redacted]	
Smith, Brittany	Undergrad Student Employee/BW			SOM: Peds: Infectious ...	britt: [redacted]	
Smith, Brittany	Patient Svcs Coord I			TEC Vas Surgery SJ	britt: [redacted]	

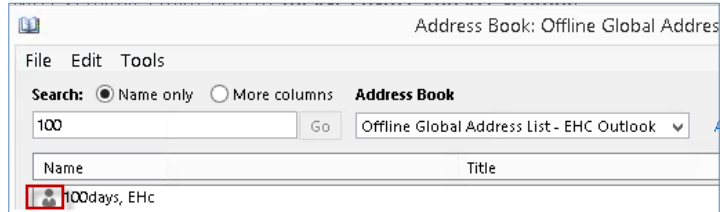
➤ If using the Emory/EHC MS Exchange email system, be aware of the following additional security features and information.

- Emails to Emory.edu addresses.
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:
 - Locate the person in the Global Address list or address book
 - Verify the icon to the left of the person's name:

If it is a person icon



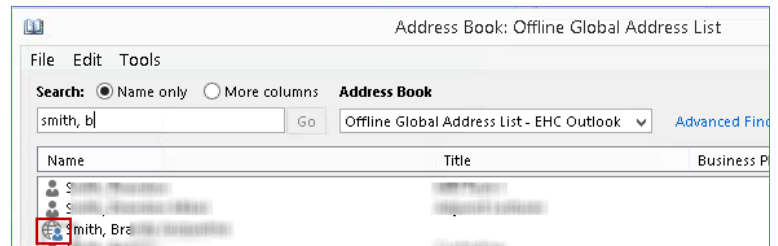
then the email is secure and it is OK to email this person.



If it is person in front of a globe



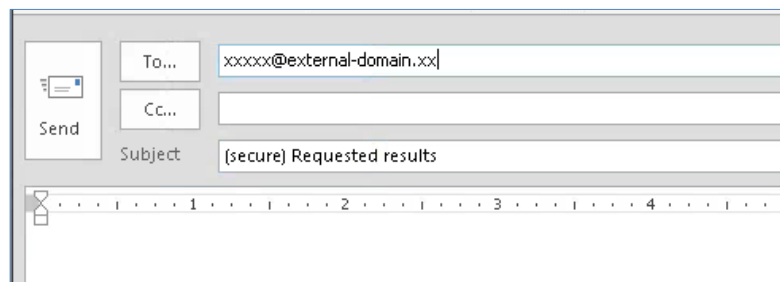
DO NOT send the user any emails containing ePHI or sensitive information unless it is otherwise encrypted.



Hint: the globe icon indicates the email address is external to or outside EHC/Emory University.

- **Encryption of Outgoing External Emails**
 - EHC uses Office 365 Message Encryption (OME) to encrypt outgoing email messages.
 - You do not need to encrypt e-mail messages sent solely to other emory.edu or emoryhealthcare.org e-mail addresses.
 - When sending sensitive information via e-mail to external parties, you should encrypt the message. OME allows EHC 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 an external email address, you must add either **(encrypt)** OR **(secure)**, including the parentheses, or 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.

- The EHC Patient Portal should continue to be utilized as the primary method of communicating with patients. Office Message Encryption must be used when communicating with a patient via email directly outside of the Patient Portal, even if the patient has requested communications via email or initiated the email exchange.

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>.

- **Internal EHC Email**

- All emails sent between EHC (@emoryhealthcare.org) email addresses are secure!

- **Additional information about EHC Email**

- Use email in support of your job. Do NOT forward humor stories, chain letters, political or religious views, etc.
- Email belongs to EHC and must always be used consistently with EHC policies.
- Email and email attachments can be subpoenaed.
- Emails 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, even if they look legitimate. 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!

Incident Handling

- Report erratic workstation behavior or unusual e-mail messages to your department manager, EHC Information Services or EHC Service Desk.
- Report any suspected issues or incidents to a manager or the EHC Service Desk.
- Report lost or stolen EHC issued devices to EHC Service Desk and the Emory Police Department and, when appropriate, to the local police.
- EHC Service Desk can be contacted at 404-778-4357.

Patient Privacy 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.
- 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
 - Ranging from \$127 to in excess of \$1,500,000.
- 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 of employment or other EHC relationship.



Acknowledgement of Privacy and Security Awareness Training

Scope:

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 EHC information technology devices or systems that may include ePHI and PHI in any other medium and I hereby certify that:

1. I have read and understand the EHC “Privacy and Security Awareness Training” handout.
2. I understand the importance of maintaining the confidentiality and integrity of all ePHI and PHI.
3. I understand that it is against EHC policy to access my PHI and ePHI through EHC Systems including the EeMR except as permitted for patients generally (for example, using the EHC patient portal). I also understand that it is against EHC policy to ask another employee or provider with access to the EeMR or other EHC Systems to access my PHI and ePHI.
4. I agree to abide by the EHC policies and procedures, as further explained in the EHC “Privacy and Security Awareness Training” handouts.
5. I understand that, by not following EHC 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.
6. I understand I can call 404-778-2757 if I have questions regarding the training or EHC policies or procedures related to PHI/ePHI I agree to call this number if I have any question regarding the “Privacy and Security Awareness Training. When in doubt reach out!

SIGNATURE and AFFILIATION

DATE

PRINT NAME

DEPARTMENT/SECTION

INSTRUCTIONS FOR COMPLETING AND RETURNING FORMS:

- If you are accessing and signing these Terms within the EHC New Applicant System, the signed Terms will be automatically sent to EHC following signature.
- If you are requesting Emory Healthcare Link (EpicCare Link) access, you must attach these signed documents to your Emory Healthcare Link access request.
- If you are requesting EpicCare (Epic Hyperspace) access, you must attach these signed documents to your EpicCare access request.
- Otherwise, you must sign and date the Terms, and **email the scanned signed and dated Terms to your access coordinator.**
- You may contact your Access Coordinator with questions regarding logon ID access.
- **DO NOT FAX THIS** form to the EHC Office of Compliance Programs.
- Please note that the signed and dated Confidentiality and System Access Terms must also be received by EHC before access may be granted.