What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) is well known in healthcare. These federal regulations create requirements for covered entities to protect the Privacy and Security of patients’ health information. They also grant patients specific rights in regards to the use and disclosure of their health information.

HIPAA applies to all healthcare providers, healthcare clearinghouses and health plans (covered entities). It protects all information obtained about a patient, often referred to as PHI (Protected Health Information).
HIPAA Enforcement

HIPAA is enforced by the Office for Civil Rights (OCR), a division of the Department of Health and Human Services.

All HIPAA violations requiring notification to the individuals must be reported annually to OCR.
The information protected by HIPAA is known as Protected Health Information (PHI). PHI can be in any form; written, electronic, or verbal and includes:

- Clinical Information
- Demographic Information
- Financial and Billing Information
- Identifying Someone as a Patient
- Health Plan Member Benefit Information
EvergreenHealth has developed HIPAA Privacy & Security policies to protect all types of personal and confidential information as required by both federal and state regulations.

Protecting information is everyone’s responsibility.

These policies can be found in Lucidoc under Compliance, Ethics and Quality/HIPAA.
Protecting Information

While HIPAA may focus on PHI, EvergreenHealth’s Privacy and Security policies help us to safeguard all of our information, including:

- Financial
- Payroll
- Human Resources
- Health Benefits
- Other types of sensitive information, including business proprietary, regulated and confidential
Facility Directory

The facility directory includes the location of all patients who are placed in a bed within EvergreenHealth such as: inpatients, emergency department, day surgery, etc. This information is available to callers and visitors who ask for a specific patient by name.

Patients have the right to opt out of inclusion in the facility directory.
NIK = No Information Known

A patient that has requested not to be included in the directory will be listed in Cerner as NIK. Or No Info.

Additionally, they will be listed on the patient tracking boards with a yellow star:

Remember: NIK = No Information Known. The presence of the patient in our facility cannot be disclosed.
Use and Disclosures of PHI

We MAY use PHI for treatment, payment or health care operations without patient authorization.

We MAY disclose PHI if required by law or for public health/health oversight without patient authorization.

In general, any other use or disclosure of PHI outside of the above parameters requires authorization and permission from the patient.
We may NOT disclose PHI to an individual whose identity and authority to receive the information is not known to us. The individual’s identity and authorization must be verified.

All routine release of information requests should be sent to Health Information Management for processing.

Any phone request must be followed with a fax request containing appropriate identifiers to verify the authority of the requestor before PHI can be shared.
HIPAA requires that uses and disclosures of PHI involve only the Minimum Necessary information to fulfill the purpose of the request.

WA State law has an equivalent provision, called “Need to Know”, which also applies to information shared between providers.

When responding to a request for information, only the minimum amount necessary to fulfill the purpose of the request may be disclosed.*

*To ensure appropriate disclosures, all routine requests for information should be referred to HIM.
Incidental disclosures occur when PHI is disclosed in violation of the “need to know” or Minimum Necessary rule. HIPAA permits certain incidental disclosures that occur as a by-product of another permissible or required use of the information.

EvergreenHealth must apply reasonable safeguards and disclose only the minimum amount of PHI necessary to accomplish the purpose of the communication.

Ways you can minimize incidental disclosures:
• Don’t leave charts open in patient care areas
• Avoid discussion of patient care in public areas
• Pull curtains in semi-private rooms/treatment areas
EvergreenHealth staff may only access information that is directly related to the performance of their jobs. Outside of your job responsibilities, you cannot access information.

*For example, you may have access to patient information, but you may not access information out of curiosity, such as checking to see if a neighbor, relative or co-worker was admitted to the hospital or their condition. Contact the Operators for this information.

You cannot access your own information or information for your family even if they have asked you to. Refer them to their provider or HIM to obtain copies.
Faxing of PHI

EvergreenHealth allows faxing of PHI for continuing care ONLY.

- Do not fax to school, work, or personal numbers.
- Verify your fax number before sending. Use preprogrammed fax numbers when available, but check them periodically.
- Use the approved EvergreenHealth fax coversheet. No PHI is allowed on the coversheet.
- If you receive a mis-directed fax containing PHI, notify the Privacy Office and send a copy to MS #49.

Faxing Protected Health Information policy
Be very careful about what you post on the internet!

• You may not post or link photos, videos, audio recordings or identifying descriptions of EvergreenHealth patients on any social media.

• Do not cite or reference business associates or co-workers on social media without their approval.

• Any information that can identify a patient is protected by HIPAA. Even if you don’t mention a name, other details may allow others to identify the individual.
Texting of PHI

Text messages are inherently insecure and can expose EvergreenHealth to potential privacy and security violations.

Additionally, text messages are not captured within the medical record.

Texting of Protected Health Information is not allowed at EvergreenHealth.
Photography

Pictures can only be taken for the purpose of treatment unless the patient signs an authorization.

Pictures should be taken on EvergreenHealth owned devices, not personal cellphones or cameras.
Notice of Privacy Practices

We are required to provide patients with a copy of the EvergreenHealth Notice of Privacy Practices which outlines our use and disclosure of PHI. It also provides information about the individual rights that HIPAA grants to patients. These rights affect employee responsibilities and include:

- Right to Request Restriction
- Right to Request Confidential Communications
- Right to Request Access to their Medical Record
- Right to Request Amendment
- Right to Request Accounting of Disclosures
Patients have the right to request a restriction on the use and/or disclosure of their PHI. We are not required to agree to the restriction. In many cases doing so could negatively impact patient care or safety.

Requests must be in writing and routed to Health Information Management (HIM) for processing.
Right to Request Confidential Communication

Patients have the right to make special requests relating to how their PHI is communicated to them.

For example, a patient may request that she receive appointment reminders at work instead of at home.

HIPAA requires us to accommodate these requests, if reasonable.
Patients have the right to request access to their own medical records. They may request to receive copies, or to review the information. If they wish to review the information, an EvergreenHealth representative must be present.

Requests must be in writing and routed to HIM for processing.
Patients have the right to request amendments to their own medical records. The request must be in writing. We are not required to agree with the amendment request. The provider involved will be consulted and an appropriate note placed in the chart. If the amendment is denied, the patient has the right to include a note in their chart.

The Amendment form can be found on our website at: https://www.evergreenhealth.com/medical-records

Requests must be in writing and routed to HIM for processing.
Right to Request Accounting of Disclosures

Patients have the right to request a list of all the times that their PHI was disclosed not for treatment, payment, healthcare operations or from a signed authorization, with a few exceptions, within the last 6 years.

Requests must be in writing and routed to HIM for processing.
Because patients have the right to request an Accounting of Disclosures, we are required to track disclosures of PHI.

At EvergreenHealth, the Health Information Management (HIM) Department is responsible for releasing PHI and tracking all disclosures.
EvergreenHealth Security
Information Security

In Healthcare, the Confidentiality, Integrity and Availability of information is critical.

Accordingly, it is everyone’s responsibility to learn and practice processes which promote this.

By following good security practices you help to ensure that our information remains secure.
We protect information from three different perspectives:

**Confidentiality**: Ensuring that information is not accessed by unauthorized persons. We take steps to protect our information from external and internal threats.

**Integrity**: Ensuring that information is not altered by unauthorized persons. This means that the information you need to do your job is accurate.

**Availability**: Ensuring that information required is readily available to authorized persons. This requires measures to increase the reliability of our electronic systems to minimize downtime.
Classification of Information

EvergreenHealth classifies information into three categories to assess the appropriate security controls to protect the information based on the classification.

1. **Confidential:** Information that is very sensitive in nature and typically subject to federal or state regulations. Unauthorized disclosure of this information could seriously and adversely impact EvergreenHealth.

2. **Restricted:** Information that is circulated on a need-to-know basis or sensitive enough to warrant careful management and protection to safeguard its integrity and availability, as well as appropriate access, use, and disclosure.

3. **Public:** Information that is published for public use or has been approved for general access by the appropriate EvergreenHealth authority.
Sources of Threats

Internal
- Unintentional – Employees acting mistakenly in good faith
- Intentional – Disgruntled or unhappy staff
- Poorly configured/designated systems

Environmental
- Natural disasters (flood, fire, earthquake)

Outsiders
- Ex-employees
- Hackers
- Viruses/Malware
Safeguards

We safeguard our information against these threats by implementing standard information safety protocols. These include:

• Individual login IDs and passwords
• Using shred bins to dispose of confidential information
• Appropriately disposing of CDs and other mediums containing confidential information
• Discussing confidential information only in private settings
• Quickly retrieving printouts from shared printers, particularly when the material includes confidential information
• Restricting use of USB drives on many workstations and encouraging use of encrypted USB drives when in use
• Setting automatic screen-locks and application timeouts on workstations
• Encrypting data on EvergreenHealth laptop’s hard drives
Use of Email

EvergreenHealth provides employees with an email account that should be used for work purposes only.

*The organization reserves the right to review any email you send or receive; There should be no expectation of privacy.

*Do not send any emails with offensive language.

*Never send an email containing confidential information or PHI outside of the organization without encrypting. This is done by adding \(<SPACE>_s\) to the end of the Subject line: e.g. Subject: Financial Reports _s

*Emails sent outside the organization are automatically scanned for profanity and for Confidential information (PHI, credit card no’s, etc.); as a result they may be blocked or sent out encrypted with a copy to the Privacy Officer.
Email Filtering

Just like with regular mail you get in your mailbox at home, junk email (spam) is also a fact of life with email. However, spam can be much more dangerous as it is a common method used to deliver malware to your computer. Most of the serious malware incidents we have been hit by over the years at EH were caused by malicious spam, including the Feb 2016 incident when we had to shut down our email system for three hours.

To help deal with this unwanted junk mail, both malicious (containing malware) and just annoying (marketing emails for example), EvergreenHealth uses mail filters to block the majority of it before it reaches your Inbox.

On average, about 80% of email incoming to EH is blocked before it hits a user’s mailbox. If we were to stop using mail filters every user’s mailbox would very quickly be flooded with junk mail.
Email Filtering

Our mail filters are extremely accurate, but mail-filtering is not an exact science. We will occasionally have some emails get through which should have been blocked, and some emails which get blocked which should have been delivered.

If you feel that a legitimate email has been blocked by the mail filters:
• Submit a Helpdesk ticket by the usual phone or email methods, ideally stating the Sender’s email address.
• IT will look into the mail filter logs and if it is blocked will deliver it to you.
• We can also whitelist specific Sender addresses you regularly get work-related email from, and similarly we can whitelist emails by specific phrases in the Subject line.
  – Note: we cannot whitelist entire email domains (e.g. @gmail.com) as this is a security risk and defeats the purpose of having mail filters
Spam - Precautions

*DO NOT OPEN attachments or click on web links in emails unless you are very sure the email is legitimate; it should be related to something you are working on with the Sender.

*Be particularly careful when you receive an email with attachments or a link to a website. Even if it seems to be from a work colleague, be suspicious. Ask yourself: ‘Would this person really be sending me an email such as this? Is it related to something I am working on with this person?’

*If you have any doubts, give the person a call and check if they did send it to you.

*Also be careful when reading email on your smartphone, as on the small screen it can be harder to notice spam email and click on dangerous links without realizing.
If you believe you have received a malicious/spam email:

• **DO NOT** click on any links in the email.
• **DO NOT** open any attachments that arrive with the email.
• **DO NOT** reply to the email or attempt to contact the senders in any way.
• **DO NOT** supply any personal information of any kind as a result of the email.
• **REPORT** the spam email by forwarding (without any attachments) to helpdesk@evergreenhealthcare.org, then DELETE it.
• Please **be selective** when giving out your EvergreenHealth email address, as the more places such as websites that you enter it the more likely you are to receive spam.

If you did open one of these emails and opened the attachment also, please submit a Helpdesk ticket stating this and your workstation number.
Web Filtering

EvergreenHealth provides access to the Internet which should be used for work purposes.

* Web usage by employees is monitored and logged, there should be no expectation of privacy for Internet use by staff.

* Access to various websites is filtered, meaning that certain categories of webpage are blocked, e.g. Porn sites, Social media sites, and also for security reasons sites which can be used to transfer data out of the network such as Online Storage (e.g. Dropbox) and Webmail (e.g. Gmail).

*If you need access to a blocked website for a work-related purpose please submit a helpdesk request by email to: helpdesk@evergreenhealth.com
One of the most common mistakes we see with computer use at EvergreenHealth is workstations left unattended while logged in. This happens both on the main campus of the hospital and at clinics. Leaving the workstation unlocked leaves highly confidential data, such as patient info, available to anyone who walks by.

This is a significant security risk, making it easy for someone with malicious intent to cause serious damage. The person that would likely be blamed for this damage is the user that left their workstation open and unattended. The repercussions to the user could be quite severe.

The good news is this is a huge problem with a very simple solution:

**Lock Your Workstation**
Kiosk Workstation which DOES NOT require login to reach desktop:

• This type of workstation normally has a name beginning ‘WSKxxxx’ or ‘WXxxxxx’, and is generally found in Clinical areas, exam rooms, etc...

• The user for a kiosk workstation will usually be a clinical staffer such as a MA, Nurse or a Physician. These workstations are generally shared among many different staff, whoever happens to be on shift at the location.

• These workstations cannot be locked at the Windows desktop, but they are generally used to display PowerChart, so the screen is often showing very sensitive patient information.

To lock these systems, please use the ‘Change User’ option within PowerChart:
How to Lock – TITO Workstations

TITO (Tap-in/Tap-Out) Workstation:
• This type of workstation normally has a name beginning ‘WVDxxxxx’
• It’s very easy to lock these workstations: just tap the sensor with your keycard and it’s done! Tap again to log back in.
How to Lock – Regular Workstations

Regular Workstation which requires login to reach desktop:

• This type of workstation normally has a name beginning ‘WSxxxxx’ or ‘WSLxxxxx’ (laptop)
• It’s very easy to lock these workstations: just hold down the ‘Windows’ key (to the left of the ALT, next to the Space bar) and press L.

• Alternatively you can press [CTRL]-[ALT]-[DEL] then [Enter]. Either way it will quickly lock the screen and no-one can access until you login again.
This is a reminder of the importance of strong passwords in securing access to systems using your login, not just for EvergreenHealth but for all your logins.

- Do not use the same password for access to EvergreenHealth’s network that you use for anything else. In fact for good password security in general you should separate all your logins which require passwords into a number of categories, e.g. Work, Banking, Medical, Social Media, Low Risk (e.g. rewards programs for a supermarket), and use different passwords for each. Even within a category use slight variations in your passwords which differentiate between them.

- Instead of basing your password on a word, e.g. Seahawks99!, base your password on a phrase you will remember easily, and use the first character of each word, e.g. I Want 2 Watch Seahawks In The Superbowl! would be ‘Iw2wSits!’.

Password Tips
Password Tips

• Use long passwords; we recommend at least 10 characters. A modern processor running a brute force cracking program could crack a six character password in 500 seconds, seven letters (13 hours), and eight characters (57 days). So the longer the better.

• Change your passwords regularly. Some systems such as Evergreen network logon will remind you to change your password after a certain interval (120 days). For other systems which don’t, do it manually.

• Don’t write down your Work or Banking passwords anywhere. For other categories you might not use very often, store them in a specialized password storage app on your smartphone, e.g. Dashlane.
Password Tips

• Make sure access to your smartphone is protected by a PIN/password/fingerprint and set it to lock after a couple of minutes of inactivity.

• Never give your passwords to anyone. Support staff will not ask you for your password and you certainly should never be emailing them to anyone in response to a query.

• If you ever suspect your password has been compromised, change it immediately. If it’s your EvergreenHealth password you should also alert Helpdesk (x1740).
Healthcare organizations have become a prime target for hackers in the last few years. Some of the common threat strategies staff should be aware of are:

- Social engineering
- Phishing
Who are Social Engineers?

Social Engineering has become one of the leading methods of compromising network security. They use manipulation of people, as opposed to using computer systems, to gain access to information.

They may call pretending to be the IT Service Desk and ask for your password to verify that you have access, while in fact they intend to use your password to gain access to our systems.

Another common trick is Phishing
What is Phishing?

Phishing is the use of an email or website to attempt to trick someone into:

- Providing sensitive information (user name, password, payment card details, etc...)
- Clicking on a link or opening a file that introduces malware
Common Examples of Phishing

Vendor – email accounts of a supplier are spoofed or hacked. An email is received requesting a wire transfer for an invoice payment to an alternate account.

Executive Suite – email accounts of executives are spoofed or hacked. A request for a wire-transfer is sent from the compromised account to staff that would normally process those requests.

Personal – you receive an email with a fax that you had not requested or were not expecting.
How to Spot a Phishing Email

- The message contains a misleading URL
  - ex: billgates@micr0soft.com
- The message contains poor spelling or grammar
- The message was unsolicited
- The message includes suspicious attachments
  - Ex: .scr, .bat, .exe
- Or something just doesn’t look right
Sanctions

The sanctions allowed for violating HIPAA policies can be severe. Failing to abide by EvergreenHealth’s Privacy and Security policies can result in:

• Lawsuits against you and the organization
• Termination of employment
• Prison sentences
• License sanctions
• Maximum penalty of $1.5 million per violation
Criminal Penalties

Covered entities and specified individuals whom “knowingly”, as explained below, obtain or disclose PHI in violation of HIPAA face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to ten years.

The Department of Justice (DOJ) interpreted the definition of “knowingly” as requiring only the knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.
EvergreenHealth expects all workforce members to report suspected Privacy or Security violations or any concerns about Privacy or Security practices.

Retaliation against any person who reports or files a Privacy, Compliance or Security complaint is not allowed per HIPAA.

If you wish to remain anonymous in filing your complaint, please call our Compliance Hotline: 425-899-5599
Privacy and Security issues should first be reported to your manager. It is important to keep your manager informed of issues in your work area.

EvergreenHealth Corporate Compliance, Information Security & Internal Audit Officer:
Richard A Meeks, CHC, CCEP, CHP
RAMeeks@evergreenhealth.com
425.899.2011