Footnote:
MedStar Health, Inc., as the parent company, is located in Columbia, Maryland. In addition, the system is made up of a number of wholly owned subsidiaries, including Franklin Square Hospital, Georgetown University Hospital, Good Samaritan Hospital, Harbor Hospital, MedStar Physician Partners, MedStar Research Institute, National Rehabilitation Hospital, Union Memorial Hospital, VNA, Washington Hospital Center, and MedStar Health Diversified businesses. While these businesses operate independently of one another and as separate employers, they also work toward common missions and values, with the ultimate goal to be the healthcare provider of choice in the Baltimore-Washington region. In working to achieve this goal, it is the responsibility of each subsidiary to enforce its privacy policies and to take appropriate disciplinary or other actions for employee violations. Please note that for purposes of this Protecting Patient Privacy training booklet, the MedStar Health parent company and all of its subsidiaries will be referred to collectively as "MedStar Health." For Privacy Rule purposes only, MedStar Health is organized as an Affiliated Covered Entity, as described in 45 CFR § 164.504(d)(1); legally separate entities that are affiliated may designate themselves as a single covered entity.
# Table of Contents

**What you will learn in this course** .................................. 1
  Function Specific Technical Fact Sheets .......................... 2

**Introduction** ............................................................ 3
  Non-Compliance Consequences ................................. 3

**MedStar Health Privacy and Security Offices** ............. 4
  How to Contact the Privacy or Security Officer .............. 4
  Concerns/Complaints/Disciplinary Actions ....................... 5

**Protected Health Information** ................................. 6
  What is PHI? .......................................................... 6
  What is ePHI? .......................................................... 6
  PHI and ePHI Identifiers ........................................... 7
  Protecting PHI ......................................................... 8

**Notice of Privacy Practices** ...................................... 9

**Using and Disclosing PHI** .......................................... 10
  Verification and Minimum Necessary ........................ 10
  Patient Authorization for Release of PHI .................... 12
  Permitted Disclosure of PHI .................................... 14
  Incidental Disclosure of PHI .................................. 15
  Disclosure to Family and Friends ............................... 17
  Disclosure for Patient Directories ............................ 18
  Disclosures to Business Associates ........................... 19

**Patient Privacy Rights** ............................................. 20
  Right to Obtain a Copy of Our Notice of Privacy Practices .. 20
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to File a Complaint</td>
<td>20</td>
</tr>
<tr>
<td>Right to Request Restrictions On Certain Uses and Disclosures</td>
<td>20</td>
</tr>
<tr>
<td>Right to Select How to Receive Health Information</td>
<td>21</td>
</tr>
<tr>
<td>Right to See and Copy Records</td>
<td>21</td>
</tr>
<tr>
<td>Right to Update Records</td>
<td>22</td>
</tr>
<tr>
<td>Right to Obtain a List of Disclosures</td>
<td>23</td>
</tr>
<tr>
<td><strong>Safeguarding Electronic Information (ePHI)</strong></td>
<td>24</td>
</tr>
<tr>
<td>Passwords</td>
<td>24</td>
</tr>
<tr>
<td>Data Access</td>
<td>25</td>
</tr>
<tr>
<td>Remote Access</td>
<td>25</td>
</tr>
<tr>
<td>Audit Trails</td>
<td>25</td>
</tr>
<tr>
<td>Email, viruses, and other outside threats</td>
<td>26</td>
</tr>
<tr>
<td>Physical Security</td>
<td>27</td>
</tr>
<tr>
<td><strong>Applying This Course to Your Job</strong></td>
<td>28</td>
</tr>
<tr>
<td><strong>Conclusion</strong></td>
<td>29</td>
</tr>
</tbody>
</table>
WHAT YOU WILL LEARN IN THIS COURSE

In this course, we will teach you about our policies and procedures regarding the privacy and confidentiality of patient information. You will learn about:

◆ The MedStar Health Privacy Office and Security Office—where to go with questions and concerns
◆ Protected Health Information—what exactly is protected information (PHI)? What is Electronic Protected Health Information (ePHI)?
◆ Notice of Privacy Practices—the publication we give to patients explaining how we use and disclose their health information.
◆ Using and disclosing patient information—authorizations, requestor verification, release of minimum necessary information, incidental disclosures, disclosures to family, friends and for patient directory, and business associates
◆ Patient Privacy Rights—patient rights in controlling how their health information is shared and communicated
◆ Safeguarding electronic patient information (ePHI)—making information secure but readily accessible
◆ Complaints and Disciplinary Actions—how to report complaints, assurance that reporters will not be penalized, potential disciplinary actions of employee non-compliance
◆ Patient Privacy Application—How to apply what you have learned here to your specific job
Function Specific Technical Fact Sheets

If your job requires more detailed information than this course provides, your supervisor will provide you with HIPAA Privacy Technical Fact Sheets designed to give you more information about privacy procedures specific to your job functions. Your supervisor will decide if you need a HIPAA Privacy Technical Fact Sheet, and will explain any Technical Fact Sheet that you will be using.

If you are an IS system administrator who requires more detailed security information, please contact the MedStar Security Officer (see page 4).

Look for shaded boxes like this for Frequently Asked Questions. These boxes explain how to apply our privacy policies and procedures to how you do your job.

Look for this clipboard for important notes and reminders.
INTRODUCTION

You have probably been working with patient privacy and accessing patient (or confidential) information in your job. You may feel you know quite a bit about privacy and security, and chances are you do.

“Patient First” is the heart of quality care at MedStar Health. Part of “Patient First” is our promise to keep patient information private. Until now, this promise was part of our Code of Conduct and state law. Now, it is national law.

Patient Privacy Is Now National Law. These new national laws, called the HIPAA Privacy Rule and the HIPAA Security Rule, and our state laws regulate what we may and may not do with patient information.

- The HIPAA Privacy Rule also grants new civil rights to all patients in the form of Patient Privacy Rights.
- The HIPAA Security Rule addresses the securing of electronic Patient Health Information (ePHI).

Non-Compliance Consequences

The HIPAA Privacy Rule enforcement date is April 14, 2003. The HIPAA Security Rule enforcement date is April 25, 2005. The implications of non-compliance are very serious. We have modified our policies and procedures to further protect patient privacy, and to comply with the new laws.

Not complying with the new laws could mean:

- Lawsuits against the hospital or MedStar business
- Fines up to $250,000
- Up to 10 years in prison
- Disciplinary action, including possible loss of your job
- Bad press about the hospital or business
- Unhappy patients
MedStar Health Privacy and Security Offices

MedStar Health has a Privacy Officer to make sure that our patients’ health information is kept private. The MedStar Privacy Officer is in charge of policies and procedures to protect patient privacy. Additionally, the Privacy Officer resolves complaints about how we keep patient information private, including both employee and patient complaints.

Also, MedStar Health has a Security Officer who is responsible for all aspects of compliance with the Security Rule. The MedStar Security Officer is in charge of resolving instances of inappropriate access to ePHI including loss or theft of PDAs or laptops containing ePHI.

How to Contact the Privacy or Security Officer

To notify the MedStar Privacy or Security Officer of a concern or complaint, or if you have a question about our privacy or security policies and procedures:

Telephone: 1-877-277-4822 (toll free)
Email: PrivacyOfficer@MedStar.net
Email: SecurityOfficer@MedStar.net

Remember: All patient or employee complaints about our privacy practices must be reported to the MedStar Privacy Officer. Patient or employees complaints about security practices must be reported to the MedStar Security Officer. The toll-free number listed above can be used to report either Privacy or Security complaints.
Concerns/ Complaints/ Disciplinary Actions

You are expected to report a concern if you see anything that you think violates our Privacy or Security policies and procedures. Tell your supervisor about your concerns. Your supervisor is expected to report them to the MedStar Privacy or Security Officer. If you don’t want to report your concerns to your supervisor, communicate directly with the MedStar Privacy or Security Officer.

Remember: Each of us has the responsibility to make sure our patients’ health information remains private. Anyone found violating the privacy of our patients may be appropriately disciplined.

Q. Will I get into trouble if I report someone breaking the rules?
A. MedStar Health wants you to report any problems you see. The MedStar Health non-retaliation policy means that you will not get into any trouble for reporting these problems in good faith. You can make an anonymous report by calling 877-277-4822.

Q. What if my laptop or PDA is lost or stolen?
PROTECTED HEALTH INFORMATION

Each MedStar hospital and health care business receives and manages health information about our patients. This information, now protected under national law, is called “Protected Health Information,” or “PHI.”

Even if you seldom use PHI in your daily job activities, it is all around you. You need to be very good at keeping PHI safe, so it doesn’t get out where it doesn’t belong!

What is PHI?

PHI can be in any form, such as:

- Patient medical record
- Patient information in electronic form (ePHI)
- Telephone calls and voice mail about patients
- Fax transmissions that contain patient information
- Emails that contain patient information
- Conversations between clinical staff about treating patients

Protected Health Information (PHI) is anything you see or hear that lets you know about the health of a specific patient.

What is ePHI?

ePHI (electronic Protected Health Information) is any electronic form of PHI including data stored on computer hard drives, file servers, data storage tapes and CDs. ePHI includes data transmitted electronically, including email.

Electronic Protected Health Information (ePHI) is electronic forms of PHI.
Note: Even the fact that an individual is a patient of ours, or pays us for services, is Protected Health Information.

PHI and ePHI Identifiers

Any identifier on the following list about the patient or the patient’s relatives, employers or household members is considered Protected Health Information:

- Names
- Geographic subdivisions
- All elements of dates
- Telephone Numbers
- Fax numbers
- E-mail addresses
- Social Security Numbers
- Medical record numbers
- Health plan numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers and serial numbers
- URL or IP address numbers
- Biometric identifiers such as finger prints
- Full face photographic images
- Any other unique identifying number, characteristic, or code

Note: You can “de-identify” health information by removing all of the identifiers listed above. “De-identified” information is not subject to the HIPAA Privacy Rule and can be freely disclosed.
Protecting PHI

We need to be very careful with patient health information. Patients expect us to protect their information from anyone who does not need to know it.

Protecting patient information is the responsibility of each one of us!

**Q.** What about patient information at the nursing station?

**A.** Don’t leave patient information, such as nursing care sheets, progress notes, face sheets, lab results, or prescription orders open and easily viewable to passers-by. Information needed in patient rooms should be covered to protect patient privacy. Computers are set to automatically logoff to protect ePHI.

**Note:** If you have a concern about patient privacy, or if something doesn’t seem right, ASK!!! You must go to your supervisor or to the MedStar Privacy or Security Officer for help. Contact information for the MedStar Privacy or Security Officer is located on page 4 of this document.

Remember:

<table>
<thead>
<tr>
<th>Don’t snoop</th>
<th>Don’t gossip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keep your voice down</td>
<td>Respect patient health information</td>
</tr>
</tbody>
</table>
The *MedStar Health Notice of Privacy Practices* explains to our patients what we may do with their personal health information. It tells them that we will continue using their health information, very carefully, for treatment, payment, and health care operations. It tells them that we will ask for their authorization to share their health information for reasons other than those stated in our *Notice of Privacy Practices*.

*The MedStar Health Notice of Privacy Practices* also tells each patient about his or her new civil rights, or *Patient Privacy Rights*.

We give each patient a copy of our *Notice of Privacy Practices* when we first encounter them, usually when a patient comes to a registration area.

We try to have each patient sign an acknowledgement that they received our *Notice of Privacy Practices*.

**Note**: We do not have to get a patient acknowledgement signed in emergency situations. We can wait until it is practical to give the *Notice of Privacy Practices* to an emergency patient.
PROTECTING PATIENT PRIVACY

USING AND DISCLOSING PHI

Verification and Minimum Necessary

We need to be careful with patient information. The two key rules of being careful about releasing patient information are:

- **Verify the Requester**: Before you disclose patient information, confirm that the requestor is entitled to receive it. There are many ways to verify that a person is who they say they are. For example, you can identify a patient by name and address, Social Security Number, or date of birth. A doctor’s office can be identified by name and tax ID number. A police officer or government official can be identified by a valid badge.

- **Provide Minimum Necessary Information**: Minimum Necessary Information means: tell the requestor ONLY what he or she needs to know. Do not offer additional information.

  **Note**: Minimum Necessary does not apply to disclosing patient information to providers for treatment purposes.

---

**Q.** A health insurance company requested a copy of the entire medical record on one of our patients insured by their company. Can I release the entire record to them?

**A.** The law permits us to rely on the request from the health insurance company as the minimum amount of information necessary for their purpose. Verify that the person calling is who they say they are, and that they have the authority to request the information.
## Protecting Patient Privacy

<table>
<thead>
<tr>
<th>Verify the Requester</th>
<th>Minimum Necessary</th>
</tr>
</thead>
<tbody>
<tr>
<td>◆ Perhaps we already know the requester</td>
<td>◆ Once you’re comfortable with the requester and the request, give out only what the person really needs to know</td>
</tr>
<tr>
<td>◆ Perhaps we have made a very simple check like a birthdate, date of service, Social Security Number, or photo I.D.</td>
<td>◆ Our co-workers usually only ask for what they need</td>
</tr>
<tr>
<td>◆ Perhaps we have asked for the requestor’s business telephone number and made a call-back</td>
<td>◆ Unusual requests from individuals you don’t know are risky. Limit the information you give out – no more than exactly what they are authorized to receive</td>
</tr>
<tr>
<td>◆ Perhaps we trust the authority of a co-worker or have seen an authorizing document</td>
<td></td>
</tr>
</tbody>
</table>

### Q. I work in billing and someone from radiology calls needing billing information on a patient who received a series of MRIs. Can I give out this information?

### A. Verify that the person is really from radiology. If you know the person, you don’t need to verify identity. If you don’t know the person, verify through the employee directory or a radiology supervisor. Also, verify authority to have the requested information. If co-workers say they need information for healthcare-related activities, you can generally assume they are allowed to receive it, or you can call a radiology supervisor and ask if the requester is permitted to have the information requested. Use the minimum necessary principle and give only the information requested.
Patient Authorization for Release of PHI

If we want to release a patient’s health information for purposes other than treatment, payment, and routine health care operations, then generally we must ask the patient to sign an authorization.

Q. What should I do if a physician calls and wants information about a patient?

A. A patient authorization is not needed to release PHI for treatment purposes. Verify that the physician is who he says he is, and that he is involved in the patient’s treatment. Then you can disclose the information that the physician is requesting.

Note: If you know the physician, you don’t need to verify.

Remember: Minimum Necessary does not apply to disclosures made to physicians for treatment purposes.

An authorization is specific to the particular situation for which it is being requested, and it lasts for only a limited period of time.

Some examples where authorization is required before we release a patient’s information are:

- A patient signs an authorization form to release PHI to an insurance company to obtain disability coverage.
- A pregnant patient signs an authorization to have her pregnancy status released to a business that markets infant care products.
- A researcher requests authorization from a patient to participate in a clinical trial.
Release of PHI related to some special conditions, such as mental health, alcohol, and substance abuse, and HIV/AIDS may require special authorization procedures.

Remember: A patient authorization is not needed to release patient information to a health care provider for treatment purposes.

Q. Do I need patient authorization to give PHI to an outside provider or physician so they can bill for their treatment services? For example, I frequently get calls from ambulance companies requesting patient registration information so they can bill the patient for transportation to the hospital?

A. The law permits us to disclose PHI to other providers without patient authorization to assist them with their payment. Verify the identity of the requestor and their authority to have the information, and disclose only the minimum amount of information necessary.
Permitted Disclosure of PHI

While the authorization rule covers most situations where we need to release patient information for purposes other than treatment, payment, and routine health care operations, there are some exceptions to the authorization rule for the good of the general population.

These three exceptions show situations where authorization is not required prior to releasing the patient’s information:

| Public health activities | ◆ Tracking and notification of disease outbreaks  
◆ Infection control  
◆ Statistics related to dangerous problems with drugs or medical equipment |
|--------------------------|---------------------------------------------------------------------------------------------------------------|
| Law enforcement and judicial proceedings | ◆ Medical records crucial to the investigation and prosecution of a crime  
◆ Medical records to identify victims of crime or disasters  
◆ Medical personnel reporting incidents of child abuse, neglect, or domestic violence  
◆ Medical records released according to a valid subpoena |
| Deceased individuals | ◆ PHI needed by coroners, medical examiners and funeral directors  
◆ PHI needed to facilitate organ donations  
◆ PHI provided to law enforcement in the case of a death from a potential crime |
Incidental Disclosure of PHI

*Incidental Disclosure* of PHI is defined as a secondary disclosure that cannot reasonably be prevented, is limited in nature, and occurs as a by-product of an otherwise permitted use or disclosure of PHI.

Examples of incidental disclosures that are permitted:

<table>
<thead>
<tr>
<th><strong>PERMITTED DISCLOSURE</strong></th>
<th><strong>NECESSARY CONDITIONS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of sign-in sheets</td>
<td>Provided that the sign-in sheet does not contain information on the reason for the patient’s visit</td>
</tr>
<tr>
<td>The possibility of a confidential conversation being overheard</td>
<td>Provided that the surroundings are appropriate for a confidential conversation and voices are kept down</td>
</tr>
<tr>
<td>Placing patient charts outside exam rooms</td>
<td>Provided that unauthorized public traffic is not permitted in the area of the exam rooms and face sheets are turned towards the wall</td>
</tr>
<tr>
<td>Use of white boards</td>
<td>Provided that only the minimum information needed for the purpose of the white board is used</td>
</tr>
<tr>
<td>X-ray light boards that can be seen by passers-by</td>
<td>Provided that patient x-rays are not left unattended on the light board</td>
</tr>
<tr>
<td>Calling out names in the waiting room</td>
<td>Provided that the reason for the patient’s visit is not mentioned</td>
</tr>
<tr>
<td>Leaving appointment reminder voicemail messages</td>
<td>Provided that the minimum amount of information is disclosed</td>
</tr>
<tr>
<td>Computer screens viewed by passersby</td>
<td>Provided that the workstation has been configured to minimize accidental viewing.</td>
</tr>
</tbody>
</table>
Incidental disclosures are permitted as long as we have complied with the minimum necessary requirements and have taken appropriate safeguards to protect the PHI.

**Q.** Do I have to take patients into a private room to take a history?

**A.** No. When you take a history from your patient, do what you can to protect your patient’s privacy. Speak in a low volume so others don’t overhear you or close the curtains around the patient’s bed.
Disclosure to Family and Friends

Certain disclosures are permitted, provided that we have given the patient an opportunity to object to the disclosure. These include disclosures to family and friends.

We must ask the patient if he or she objects to disclosing health information to family or friends.

If the patient objects, then we are not permitted to discuss the patient’s health condition with family or friends.

**Note:** If the patient is not able to tell us if he objects, such as in an emergency situation or when a patient is unconscious, then we must use our best professional judgment to decide whether to talk to a family member or friend.

**Q.** A friend is worried because his girlfriend is in the hospital. He asked me to find out anything I can. Should I try to find information for my friend?

**A.** No. You should not even tell him that his girlfriend is in the hospital. Tell your friend to call or visit the information desk. If the patient has agreed to have her information available, the information desk staff can give it to him.
Disclosure for Patient Directories

Certain disclosures are permitted, provided that we have given the patient an opportunity to object to the disclosure. These include disclosures for the purposes of the Patient Directory.

We must ask the patient if he or she objects to being included in the patient directory.

If the patient objects, then we can only disclose patient information for treatment, payment, health care operations and other limited purposes permitted by the law. We cannot disclose to anyone else that the patient is in our facility.

**Note:** If the patient does not object to being included in the Patient Directory, then we may only give out the patient’s location in the facility and general health condition to someone asking for the patient by name.
Disclosures to Business Associates

Sometimes we let outsiders see or use health information as part of our routine operations, such as transcription, accreditation agencies, copy services, and others who perform services on our behalf. These are our Business Associates.

Although we are directly covered by the HIPAA Privacy and Security Rules, our Business Associates are not. So, we are required to have special contracts with our Business Associates that bind them to the same privacy and security protections that we are required to give our patients.

We need to be careful about what our Business Associates do with the information we give to them by making sure we have privacy language in our contracts with them. We need to be comfortable that they are respecting the privacy of our patients’ information.

**Q.** What should I do if I give a vendor PHI to perform a service on our behalf?

**A.** A MedStar Business Associate Addendum needs to be signed by the vendor. Ask your supervisor about the vendor, or contact the MedStar Privacy Officer.

**Note:** While you are not required to monitor your Business Associates, if you think one of your Business Associates is not respecting our patients’ privacy, you must report your concern to the MedStar Privacy Officer. Contact information for the MedStar Privacy Officer is located on page 4 of this document.
PATIENT PRIVACY RIGHTS

The new HIPAA Privacy Law gives new civil rights, known as Patient Privacy Rights, to all our patients. These rights give patients more control over how their health information is shared and communicated.

Right to Obtain a Copy of Our Notice of Privacy Practices

Patients have the right to receive a copy of the MedStar Health Notice of Privacy Practices.

Right to File a Complaint

If a patient believes that their confidentiality has been breached or we have violated the law, he or she has the right to file a complaint with us, or directly with the Secretary of the Department of Health and Human Services.

Right to Request Restrictions On Certain Uses and Disclosures

Patients have the right to request restrictions on certain uses and disclosures of their health information.

- Patients can ask us to limit how we use and disclose their health information.
- The law does not require us to accept or agree to a patient’s request to restrict the use or disclosure of their health information.
- If we agree to accept the patient’s restriction, we must adhere to the agreement. If we do not agree to the restriction, we must inform the patient that we do not accept the restriction.
Q. What should I do if a patient asks me for a special restriction on how we disclose his PHI?

A. Do not accept the patient’s request. Tell the patient you will report his request to your supervisor. Your supervisor will notify the person in your facility who is in charge of managing these requests.

Right to Select How to Receive Health Information

Patients have a right to choose how they receive their health information.

- Patients can request that we communicate with them in a certain way, such as by mail or fax, or at a certain location, such as home address or post office box.
- We are required to do our best to accommodate reasonable patient requests for confidential communications.

Right to See and Copy Records

Patients have a right to read and obtain copies of their medical record.

- Patients can look at and receive a copy of certain medical and billing records.
- We can deny the request if the information is in mental health records, the information was gathered for a court of law, or releasing the information might harm the patient or another person.
- We must respond to the patient’s request within certain time periods.
Right to Update Records

Patients have the right to update their medical records.

- If patients believe that a piece of important information is missing from their medical record, they can request that we add an amendment to their medical records.
- We may deny the patient’s request to amend their medical record if the information being amended was not created by us, if we believe the information is already accurate and complete, or if the information is not contained in records that they would be permitted to see and copy.

Q. Are we required to delete information from the medical record if the patient asks us to?

A. No, we are not required to delete or blacken out any information in the medical record. If we accept the patient’s request to update their record, we are only required to add the update to the record.
Right to Obtain a List of Disclosures

Patients have a right to get a report of the disclosures we have made of their health information.

- We are not required to give the patient an accounting of the disclosures that we have made for purposes of treatment, payment, or health care operations.
- We are not required to include disclosures for which we received written patient authorization or certain other disclosures excluded by law.
- The report covers the six-year period prior to the request, but we are not required to include disclosures made before April 14, 2003.
- The report must contain specific information, including the dates, names, and information disclosed.

**Q.** Are we allowed to charge the patient a fee for preparing the accounting of the disclosures?

**A.** We are required to provide the first report in a 12-month period free, but we can charge a reasonable, cost-based fee for additional reports in a 12-month period.
PROTECTING PATIENT PRIVACY

SAFEGUARDING ELECTRONIC INFORMATION (ePHI)

The HIPAA Security Rule calls for us to take “appropriate safeguards” to protect the privacy of electronic patient information. This includes the patient information in our computer systems, laptops, PDAs, other portable computing devices, and information transmitted to others. We need to take special precautions that this information is:

- Not accessible to people not authorized to see it
- Not changed or deleted maliciously or by mistake
- Readily accessible to authorized providers

Passwords

Choose a password that is not easily guessed. Generally good passwords are at least six characters long and contain a combination of numbers and lower and upper case letters. Poor passwords include sports team names, family names and dates of birth.

- Do not write down your password
- Do not share your user ID or password. Never give your user ID or password to anyone who contacts you via the phone or e-mail. Help desk and IS support personnel should not ask you to give them your password.
- If you have to provide your password or if you believe that your password is compromised, immediately change your password and contact the Help Desk for assistance.

Q. Someone new in my department asks to share my user ID because they don’t have access. What should I do?

A. Report it to your manager and have an access request completed for the new user.
Data Access

As a safeguard, applications containing PHI or other confidential information “time out” or “auto logoff” after a predetermined period of time, generally 10 minutes. However:

- Logoff a workstation before you leave if you are using a workstation shared by other users, such as a workstation in a nursing unit.
- Consider using password protected screensavers for personal workstations.

Remote Access

Approved MedStar access methods include virtual private networking (VPN), Citrix, and secure web pages or portals. Direct dial-up to a modem connected to a server or workstation is NOT a secure or approved remote access method.

- Do not allow members of your family to use a MedStar supplied PC when working from home.
- If you use your own computer for remote access, have up-to-date virus software and preferably a firewall.

Audit Trails

Audit trails are used to monitor data access. An audit trail is a program that records who, when, and how users access data. MedStar uses audit trails in conducting investigations into potential privacy or security violations.

Q. My system automatically logs me off after 10 minutes of inactivity. Because of this, I never logoff when I leave for lunch. Is this OK?

A. No. always logoff when leaving your workstation for an extended period of time. The automatic log off function is a failsafe measure in case you forget to logoff.
Email, viruses, and other outside threats

Computer viruses are the most common external threat to ePHI. Viruses are most often transmitted via email attachments. In addition to using and keeping your anti-virus software current, here are some tips to guard against computer viruses:

- Delete suspicious email messages or emails from unknown senders
- Don’t open attachments associated with emails from unknown senders
- Document and report any suspicious activity, such as unknown programs appearing on your computer or changes in system performance
- Use only approved email and instant messaging programs

Email and electronic file transfers are widely used to share PHI with business associates and other healthcare providers.

- Use file encryption or, at least, password protect the files when transmitting them electronically.

**Q.** We routinely send files containing patient billing information to a third-party over the Internet—does this information need to be encrypted?

**A.** Encryption is the recommended method of protecting information while it is being transmitted over an open network like the Internet. Work with IS support if you have questions or concerns.
Physical Security

Follow these common sense security practices to secure ePHI:

- Store computer hardware (e.g., servers, disks and CDs) containing ePHI in secure locations.
- Retrieve and secure any document or media that might contain PHI such as reports in printers, faxes in fax machines or computer disks/CDs in computers or out on desks.
- To dispose of computers, disks, CDs and related equipment, contact your local IS personnel for the proper data removal and equipment disposal procedures.
- Lock down computers to prevent theft.
- Tilt computer screens away from public areas.

Regarding unfamiliar or unauthorized people in the area:

- Ask for ID when someone who you don’t know wants to work on a computer in your area.
- Report any suspicious persons without appropriate ID in secured or non-public areas of your facility.
- Escort visitors requiring access to non-public areas.

Regarding laptops and portable computing devices:

- Do not leave laptops and other portable devices unattended in areas accessible to the public. Use a security cable on laptops used in public areas or lock them up when they are not in use.
- Use a startup password on portable devices
- Encrypt all PHI stored on portable devices

**Q.** A computer workstation is stolen or missing from our department, what should I do?

**A.** Immediately report it to your building/hospital security office and the MedStar Security Officer.
APPLYING THIS COURSE TO YOUR JOB

When handling a request for PHI, you must always:

- Verify requestor’s identity
- Verify authority to have requested information
- Supply only minimum necessary information
- Secure ePHI

Remember: If you are using or disclosing PHI for purposes other than treatment, payment or operations, ask your supervisor if you need patient authorization to release the information.
Congratulations! You’ve successfully completed the “Protecting Patient Privacy” course. In this course you learned about:

- Contacting the MedStar Privacy or Security Officer if you need more information, or if you need to report a concern or complaint
- Patient Privacy Rights
- Protected Health Information (PHI) and electronic Protected Health Information (ePHI)
- Notice of Privacy Practices
- Using and Disclosing PHI
  - Authorizations
  - Requestor verification
  - Release of minimum necessary information
  - Incidental disclosures
  - Disclosures for patient directory and to family and friends
  - Business associates
- Safeguarding electronic Protected Health Information (ePHI)
- How this course applies to your job

We will continue to work on Privacy and Security Awareness at MedStar Health. If you have issues, concerns, or questions about patient privacy or security, please contact the MedStar Health Privacy or Security Officer at 877-277-4822 (toll free).
CERTIFICATE OF COMPLETION

This is to certify that

__________________________________  Name

__________________________________  Hospital or Business Unit

__________________________________  Department or Nursing Unit

Has successfully completed the Protecting Patient Privacy training course

on__________________________________  Date

Privacy Officer/ Security Officer
MedStar Health

__________________________________  Supervisor
Questions about the privacy or security of patient information and your job responsibilities should be directed to your supervisor, or to:

Privacy Officer or Security Officer
MedStar Health, Inc.
5565 Sterrett Place
Columbia, MD 21044

Phone: 1-877-277-4822
Email: PrivacyOfficer@MedStar.net
Email: SecurityOfficer@MedStar.net