PharMerica

Value. Trust. Performance.

HIPAA REFERENCE GUIDE

REVISED: November 26, 2013; June 2016; December 1, 2018; April 6, 2019

INTRODUCTION

What is HIPAA Reference Guide?
HIPAA Reference Guide provides an overview of PharMerica's HIPAA privacy policies and procedures ("Privacy Policies") which address the confidentiality of patients' protected health information ("PHI"). It is important that you review and understand the information in this HIPAA Reference Guide. Reviewing this HIPAA Reference Guide, however, does not replace the requirement that you must also carefully review all of PharMerica's Privacy Policies. This Reference Guide is intended to facilitate your review of the Privacy Policies and to serve as a reference guide of the key concepts of the Privacy Policies. You are responsible for understanding and complying with PharMerica's Privacy Policies in your daily job functions for PharMerica.

PharMerica Affiliated Covered Entity
PharMerica is a covered entity under HIPAA and is required to comply with HIPAA. For purposes of HIPAA compliance, entities which are under common ownership or control with PharMerica are designated a single affiliated covered entity ("ACE"). As an ACE, all of PharMerica entities are subject to PharMerica's Privacy Policies and PharMerica's Notice of Privacy Practices. Any reference to PharMerica in this document encompasses all entities in PharMerica's ACE.

PharMerica's HIPAA Privacy Office
The HIPAA Privacy Office oversees HIPAA compliance for PharMerica organization-wide and is comprised of the following individuals:

- **HIPAA Privacy Officer: Scott Dilley (502-627-7317)**
- **HIPAA Security Officer: Stephen Myers (813-240-8659)**
- **Chief Compliance Officer: Steve Lariviere (502-627-7404)**
- **Chief Legal Officer: Steve Reed (502-630-7438)**

If you would like more information about HIPAA or have a HIPAA compliance question, please contact the *HIPAA Privacy Office* via email at privacy.department@pharmerica.com or call the Privacy Officer at above phone number. It is always good to talk about any HIPAA compliance questions and clarify the questions with the HIPAA Privacy Office. The HIPAA Privacy Officer will also be happy to discuss and plan an education session to fit your specific needs. If you would like to schedule a HIPAA Privacy Refresher Training, please call the HIPAA Privacy Officer. In addition to the Privacy Officer overseeing HIPAA compliance organization-wide, each pharmacy designates a Privacy Coordinator for the pharmacy who is responsible for being the main contact with the Privacy Office.

Whom To Contact With a HIPAA Compliance Concern or Complaint?
Each Workforce member has the responsibility to make sure that our patients' PHI remains confidential. You are expected to report a concern if you see anything that you believe violates our Privacy Policies. You can report your concern or complaint by contacting:

- The HIPAA Privacy Office, via email at privacy.department@pharmerica.com or by calling the Privacy Officer at the above phone number, if you don't want to be anonymous.
- The toll-free PharMerica Hotline number at 1-800-793-7741, if you wish to be anonymous. This number is available 24 hours a day.

The HIPAA Privacy Office will investigate all complaints and work with the appropriate departments to resolve.

PharMerica's Privacy Policies
PharMerica's Privacy Policies address the requirements of the HIPAA Privacy Regulations. To ensure the Privacy Policies are available to you at all times, the Privacy Policies are posted at the Privacy and HIPAA Compliance SharePoint Site, as well as maintained in each pharmacy location. Please ask your pharmacy's Privacy Coordinator if you have questions about where a copy of the Privacy Policies is located in your pharmacy.

HIPAA BASICS

Key HIPAA Regulations:
Key Regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") are Privacy, Security and Breach Notification Regulations:

- Privacy Regulations protect the privacy and confidentiality of PHI
- Security Regulations establishes standards for security of electronic PHI
- Breach Notification Regulations requires notification to the individual, Office of Civil Rights, and media (in some cases) of a Breach of Unsecured PHI.

What is PHI?

- PHI is individually identifiable medical, demographic and financial information about a patient. Information is individually identifiable if it identifies the individual or there is a reasonable basis to believe that the individual could be identified. Examples of PHI include:
  - **Medical Information** – medications, diagnosis, physician orders, nurses' notes, dates of service, medical record numbers
  - **Demographic Information –** name, address, telephone number and date of birth
  - **Financial Information** – billing statements, account number and social security number
- PHI can be in any form. For example, PHI can be in an electronic medication dispensing record, in paper pharmacy records or in verbal discussions about patients' medications.

  - ***Note: PharMerica pharmacies receive and manage PHI about our patients. Even the fact that an individual is a patient of PharMerica, or pays us for services, is PHI.***

PHI becomes de-identified information only if it is completely de-identified. De-identification means that each identifier that could possibly identify the patient has been removed. De-identified information is not subject to HIPAA. ***PharMerica Policy # 21, Use and Disclosure of De-Identified Information*** explains which standards must be met to de-identify PHI. De-identification must ensure all patient identifiers are removed and must be coordinated with the Privacy Officer.

Who Must Comply with HIPAA?

- **Covered Entities:** healthcare providers, health plans and healthcare clearinghouses
- **Business Associates:** vendors who perform services for Covered Entities involving access to PHI

Who Enforces HIPAA?
Compliance with HIPAA is enforced by the U.S. Office of Civil Rights ("OCR"). The Attorney General of each state also has authority to bring action for HIPAA violations. Sanctions for violation of HIPAA Regulations are significant and include civil monetary penalties up to $1.5M and higher. Criminal penalties may also enforced by the U.S. Department of Justice.

What Does This Mean to Me?
PharMerica, a provider of pharmacy services, is a covered entity subject to HIPAA compliance. All PharMerica Workforce members, regardless of job title or hours worked, must safeguard the PHI of our patients and comply with PharMerica's Privacy Policies. You are expected to be able to:

- Recognize PHI and known when it is permissible to access, use or disclose PHI,
- Utilize safeguards consistent with PharMerica's HIPAA policies to reduce the risk of impermissible access to, use or disclosure of PHI,
- Comply with PharMerica's Privacy Policies.

Important: Detailed information about the HIPAA Regulations requirements is included in your LRN Training Modules, including Confidentiality Under HIPAA: Using Information and Security of Electronic Health Information Under HIPAA, as well as the LRN Resource Center and must be carefully reviewed.

PHARMERICA'S NOTICE OF PRIVACY PRACTICES

PharMerica's Notice of Privacy Practices is an important document which tells to our patients:

- How PharMerica may use and disclose their PHI, explaining that we can use and disclose their PHI as needed for their treatment, to receive payment for our services, for various healthcare operations activities and for other purposes permitted under the Privacy Regulations,
- That we will ask for their authorization to share their PHI for reasons other than those stated in our Notice of Privacy Practices,
- About PharMerica's duties with respect to their PHI,
- About their rights under HIPAA,
- How they can complain about a privacy issue.

Patients have a right to obtain a copy of our Notice of Privacy Practices. They may ask for a copy of our Notice of Privacy Practices at any time.

Important: PharMerica's Notice of Privacy Practice is posted on our website, in pharmacies and is available to patients. Please review PharMerica's Policy # 8, Notice of Privacy Practices which explains when and how we must provide Notice of Privacy Practices to our patients.

USING AND DISCLOSING PHI

What is meant by "Use" and "Disclosure"?
"Use" of PHI occurs when a PharMerica Workforce member shares PHI with another PharMerica Workforce member. "Disclosure" occurs when a PharMerica Workforce member shares PHI with someone outside of PharMerica.

HIPAA Requirements on Use and Disclosure of PHI.
HIPAA Privacy Regulations contains requirements on the permitted use and disclosure of PHI. As a general rule, unless the Privacy Regulations specifically permit a use or disclosure of PHI without obtaining a patient's Authorization, PHI **cannot** be used or disclosed without a patient's Authorization. Below is an explanation of the key concepts on use and disclosure of PHI and PharMerica's Privacy Policies addressing these requirements.

Use and Disclosure of PHI Without Obtaining A Patient's Authorization

***Treatment, Payment and Healthcare Operations*:** PharMerica may use and disclose PHI without obtaining an Authorization from a patient if the use or disclosure is for PharMerica's treatment, payment or healthcare operations purposes. This means that:

- PharMerica may use and disclose PHI as needed to provide pharmacy services to our patients. For example, a pharmacist can discuss medications with a patient's physician or with a nurse at a long term care facility.
- PharMerica may use and disclose PHI to be paid for pharmacy services. For example, PHI may be disclosed to a health plan to receive payment for medications.
- PharMerica may use and disclose PHI for its healthcare operations. For example, PHI may be disclosed for purposes of our quality assessment or licensing activities, surveys, peer review, legal services or business planning.

In addition, PharMerica may disclose PHI (a) for treatment activities of another healthcare provider, (b) to another covered entity or a healthcare provider for their payment purposes, or (c) for limited healthcare operations purposes of another covered entity if specific requirements of the Privacy Regulations are met.

Important: Please review PharMerica's Policy # 1, Use and Disclosure of PHI for Treatment, Payment and Healthcare Operations and Authorizations for Use and Disclosure of PHI, which explains the requirements for use and disclosure of PHI for Treatment, Payment and Healthcare Operations.

As Permitted by Privacy Regulations in Special Circumstances: PharMerica may use or disclose PHI without obtaining an Authorization from a patient if the use or disclosure is for certain special purposes specifically permitted under the Privacy Regulations without an Authorization. Examples include disclosures:

- To health oversight agencies (e.g., CMS, Medicaid, Board of Pharmacy, DEA) for inspections, licensure actions or audits
- To the FDA, to track FDA regulated products or enable product recalls
- For certain public health activities
- As required by law
- To avert serious health or safety threat

If PHI is to be disclosed for such purposes, it is important that the requirements of the Privacy Regulations that apply to each such disclosure be followed and that it is verified that the disclosure is also permitted by the applicable state law. ***Because these requirements must be checked for these uses and disclosures, the Privacy Officer must be consulted to approve the proposed use or disclosure of the PHI.***

Important: Please review PharMerica Policy # 4, Use and Disclosure of PHI in Special Circumstances, which explains when PHI may be used and disclosed without an Authorization.

To Patient's Personal Representatives, Family and Friends:

- PharMerica may disclose PHI to a Personal Representative of a patient because Personal Representatives are treated under HIPAA the same way as the patients. For example, a Personal Representative may ask for a copy of the patient's PHI or may sign an Authorization to disclose PHI. Personal Representatives are the individuals with legal authority to make healthcare decisions about the patient. For example, person holding a power of attorney for healthcare or a court appointed guardian. If you have any questions whether a person is a Personal Representatives, please contact the Privacy Officer.
- PharMerica may disclose PHI to a patient's family and friends who are involved in patient care and payment for the care. But, this disclosure must be the limited PHI relevant to their involvement in care and we must ask the patient if he or she objects to disclosing PHI to family or friends. Prior to speaking with a family member about the patient's medication therapy or billing, ask a patient's permission to do so. If the patient objects, then you may not discuss the patient's PHI with the patient's family member.
- If a patient is not present, you must exercise professional judgment whether a limited disclosure of PHI to a patient's family or friend which is directly relevant to such person's involvement with the patient's care is in the patient's best interest (e.g., if a person listed as the responsible party asks a question about the bill).

Important: Please review PharMerica Policy # 6, Disclosure of PHI to Patient's Personal Representatives and Family and Friends, which explains the requirements for these disclosures.

AUTHORIZATIONS TO USE OR DISCLOSE PHI

What is "Authorization"?

An Authorization is an individual's signed permission to allow use or disclosure of PHI as specified in the Authorization. An Authorization is specific to the particular situation for which it is being requested, and it lasts for only a limited period of time specified in the Authorization. For example, a patient may sign an Authorization permitting PharMerica to release PHI to the patient's employer, to a life insurance company or to a drug company for marketing purposes. A patient may revoke an Authorization at any time by sending to PharMerica a written revocation request. ***Unless a use or disclosure of PHI is permitted under HIPAA to be made without an Authorization, we must obtain an Authorization before using or disclosing PHI.***

Important: Please review PharMerica Policy #1, Use and Disclosure of PHI for Treatment, Payment and Healthcare Operations and Authorizations for Use and Disclosure of PHI, which explains the process for review and processing of Authorization.

Which Information an Authorization Must Contain?

- Description of the PHI to be used or disclosed,
- Person or organization permitted to make the use or disclosure,
- The person or entity to which the disclosure will be made,
- An expiration date or event, and
- The purpose for which their PHI will be used.
- Signature of the patient or personal representative and date
- Several additional HIPAA required statements.

If an Authorization does not contain all the required information, if it is not signed, not dated, expired or is known to be revoked, it is not valid and PharMerica **cannot** disclose PHI pursuant to such document. ***If your pharmacy receives an Authorization requesting release of PHI, please notify your pharmacy's Privacy Coordinator who will forward such document to the Privacy Officer at*** privacy.department@pharmerica.com ***for review, approval and response.***

Important: Form #1A, Authorization for Release of Protected Health Information, is PharMerica's approved Authorization form.

SPECIAL NOTE ABOUT DISCLOSURE OF PHI FOR MARKETING PURPOSES

Privacy Regulations provide patients with important controls over whether and how their PHI may be used and disclosed for Marketing purposes. PharMerica must obtain an Authorization before using or disclosing PHI for Marketing unless a communication in the form of a face to face communication made by PharMerica to the patient or a promotional gift of nominal value provided by PharMerica. An example of Marketing is when a drug manufacturer receives a list of patients from a pharmacy to send coupons for a new medication to those patients. If you have questions of whether a particular purpose of a disclosure is considered Marketing, please contact the Privacy Officer who will provide guidance.

Important: Use of Disclosure of PHI for marketing requires an Authorization. If PHI will be used or disclosed for marketing purposes, Form #1B, Authorization for Release of PHI for Marketing needs to be used. If PharMerica will receive any remuneration for disclosing PHI for marketing, this needs to be noted in the Authorization form.

DISCLOSURE OF PHI IN RESPONSE TO SUBPOENAS OR OTHER DISCOVERY REQUESTS

PharMerica may use and disclose PHI in the course of legal actions but only if the Privacy Regulations requirements are met. In some cases PharMerica receives requests for PHI in the course of legal actions to which PharMerica is not a party. In such cases, PHI may be disclosed if PharMerica receives:

- A valid Authorization from a patient permitting disclosure of PHI,
- A court order to disclose PHI,
- A qualified protective order on disclosure of PHI, or
- A subpoena to disclose PHI which contains documentation that a patient was notified of the subpoena, did not object to the subpoena and the time to object has expired.

Important: Please review PharMerica Policy # 3, Disclosure of PHI in Legal Proceedings, which explains the requirements for disclosing PHI pursuant to subpoenas and other legal process.

A response to a subpoena or a similar legal document must be coordinated with the Privacy Officer. If your pharmacy receives a subpoena or another discovery request to release PHI, please scan and email the request to privacy.department@pharmerica.com with the subject line: Record Request (Lastname)."

- The pharmacy's assigned Privacy Coordinator will be the point of contact with the requestor (law firm, records collection agency, etc.)

- The Privacy Coordinator will complete any documentation that needs to be provided with the pharmacy records and will be the Record Custodian of the records being released (this includes a "Records Authenticity Certification" or similar document such as a "No Records Certification" in the case of no records).
- The Privacy Coordinator will be responsible for obtaining the Privacy Officer's authorization to release the requested records, compiling the records at the pharmacy, and releasing the records to the requestor, as appropriate.

MINIMUM NECESSARY RULE

What Does Minimum Necessary Rule Mean?

HIPAA Minimum Necessary Rule means that PharMerica Workforce members must access, use and disclose only the minimum amount of PHI to the minimum number of people, to accomplish the task at hand. This rule applies to uses within PharMerica, as well as to disclosures outside of PharMerica or requests of PHI from other covered entities. The Minimum Necessary Rule also means that you must resist the temptation to peek. You must access and use only the PHI needed to carry out your job responsibilities for PharMerica. No matter how curious you might be regarding the health of a coworker, a friend, a celebrity, a family member or any other patient, do not access PHI unless you are authorized to do so and need access to perform your job.

Remember that you cannot access any PHI about family members, friends, or co-workers for personal or any other non-work related purposes. In the rare circumstance when a Workforce member's job (e.g. billing, providing pharmacy services) requires him/her to access medical information of a family member, a co-worker, or other personally known individual, then the Workforce member should immediately report the situation to his/her supervisor who will determine whether to assign a different employee to complete the task involving the specific patient.

Remember: Never assume you have the right to use or share PHI. Ask yourself these three questions:

1. Does the law and PharMerica's Privacy Policies allow me to access the PHI?
2. Do I need to know the PHI to do my job?
3. What is the minimum amount of information that is necessary to accomplish the task?

If you have any questions about complying with the Minimum Necessary Rule, please call the HIPAA Privacy Officer or email the HIPAA Privacy Office at privacy.department@pharmerica.com.

Exceptions to Minimum Necessary Rule

The Minimum Necessary Rule does not apply to the use or disclosure of PHI for treatment purposes (such as filling prescriptions) because healthcare providers may need access to the full record to provide quality healthcare. This rule also does not apply to a patient's access to his or her own PHI, to uses and disclosure of PHI authorized by the patient pursuant to an Authorization, disclosures to HHS for HIPAA enforcement purposes or disclosures required by law and carried out in accordance with the requirements of the applicable law.

A Note About Creating Reports from PHI: Certain Workforce members have been granted access to PharMerica's LTC/400 Data Warehouse which contains PHI. If you have been authorized to extract data from the Data Warehouse, and to create and format reports, you must be very careful about what information is included in the reports, and to whom the data is given. Remember that data extracted from the Data Warehouse or any other internal PharMerica source (such as dispensing or accounting systems) may be disclosed outside PharMerica only if the disclosure is permitted by the Privacy Regulations and PharMerica's Privacy Policies, or if the PHI has been de-identified consistent with HIPAA requirements and ***PharMerica's Privacy Policy #21, Use and Disclosure of De-identified Information***. If the information containing PHI will be used only for purposes of treating the patient, adjudicating the claim and receiving payment, or as an aid in reviewing and improving our internal operations, then it may usually be used without de-identification but must be consistent with the Privacy Regulations and PharMerica's Privacy Policies.

Important: Please review PharMerica's Privacy Policy #5, Minimum Necessary Standard for Use, Disclosure and Request of Protected Health Information, which addresses the requirements for compliance with the

minimum necessary standard.

SAFEGUARDS TO PROTECT PHI

We are all responsible for safeguarding our patients' PHI and taking precautions that the PHI is not accessible to those not authorized to see it. The safeguards are required regardless of whether the PHI is in paper or electronic records, in verbal discussions or visual representations. Many incidents are preventable and care must be taken to prevent improper use or disclosure of PHI.

Safeguard PHI in Paper Documents

- Do not leave paper records containing PHI in plain sight on desks when you are not working on such documents.
- Check fax machines, printers, copiers, and mailboxes frequently to retrieve PHI.
- When corresponding with patients by mail, send correspondence containing PHI in sealed envelopes.
- When sending medications to patients by mail, verify that correct medication is being sent to a correct patient
- When providing documents with PHI to a patient, check to ensure you are giving the correct documents to the correct patient (e.g., pharmacy inserts)
- All paper documents containing PHI must be shredded prior to disposal. Paper records must be disposed only to containers designated for documents containing PHI and marked to indicate that the documents are to be shredded prior to disposal.
- Do not dispose medication containers, IV bags and any other materials containing PHI in any publicly accessible recycling or trash containers unless the PHI has been removed and shredded prior to disposal.
- Printers and copiers shall be located in areas not accessible to unauthorized personnel.
- Access to areas where paper records containing PHI are stored shall be restricted and limited to authorized personnel.

Safeguard PHI in Visual Representations

- Turn your computer screen away so that screens are not visible to passers-by.
- If PHI is frequently displayed on your screen, install a "privacy screen" to protect the display.
- Computer screen savers shall be set for quick intervals.
- Sign off the computer when away from the computer and do not leave computers unattended when signed on.

Safeguard PHI in Verbal Communications

- Avoid discussing PHI in public areas, including talking on the phone where others may overhear.
- When discussing PHI, make efforts to minimize risk of being overhead by non-authorized individuals (e.g., use lower voice, hold a conversation in an enclosed area with the doors closed, etc.)
- Remember that only minimal amount of PHI may be left in voicemails and no sensitive PHI shall be left in voicemail boxes or answering machines.

Safeguard PHI in Electronic Communications
Faxes:

- Always double check the fax number before sending a fax.
- Periodically validate pre-programmed fax numbers and remind regular fax recipients to provide notification in the event their incoming fax number changes.
- Use a cover sheet with a confidentiality statement when transmitting faxes containing PHI.
- Notify the intended recipient that information containing PHI is being delivered via fax and do not fax PHI unless the recipient confirms that providing PHI via fax is acceptable to the recipient.
- Place fax machines in secure areas and promptly pick up documents from fax machines.
- If a fax is sent to the wrong recipient in error, contact the wrong recipient immediately and ask that the materials be returned or destroyed. You must also immediately notify the HIPAA Privacy Officer of the incident via e-mail at privacy.department@pharmerica.com, who will take additional actions as appropriate.

E-Mail:

- Always double-check the e-mail address before sending an e-mail message to ensure it is going to the right party.
- Do not rely on the Microsoft Exchange functionality to accurately auto-fill or auto-populate the address lines. Instead, use the Microsoft Exchange address book and select the name of each intended recipient.
- Do not send PHI to patients via e-mail unless the patient requests that or consents to receive PHI via e-mail.
- If an e-mail must be sent to a distribution list, verify the names on the list and confirm that each recipient has a need to receive the e-mail.
- Use Secure File Transfer to send large files securely to both internal and external addresses.
- If you send an e-mail containing PHI to the wrong addressee, report the error immediately to your supervisor and Privacy Officer.
- Be vigilant of suspicious e-mails, do not click on links or open documents from unknown senders, and direct any questions regarding such e-mails to IT Helpdesk
- Never provide your user ids or passwords in response to any e-mails and direct your questions regarding such e-mails to IT Helpdesk. Keep in mind that Information Technology will never ask you to disclose passwords, social security numbers or other sensitive information via email.
- Send all e-mails containing PHI only via secure encrypted e-mail, unless a patient requests access to PHI via e-mail and requests that PHI be transmitted to the patient via unsecure e-mail after being warned of the risks to PHI due to such transmission.

How to Send an Encrypted Email? *To encrypt an email, type the phrase in "**PHI Confidential**" or **"PHI Secure"** (without quotes) anywhere in the subject line. This will cause the e-mail to be encrypted before being sent to the recipient.*

How Will the Recipient Decrypt My Email? *If the recipient's email system is configured to receive encrypted email, it will decrypt the email seamlessly without any action by the user. If the recipient's email system is not configured to receive encrypted email, the recipient will receive an email stating that they have a secure message (see image below). To view the message, the recipient will be prompted for a user id and password. A registration process is required for first-time users. The message will open in a secure web portal.*

What if I Want the Recipient Go directly to Portal to Retrieve My Email? *You can do this by entering the phrase "PHI Portal" anywhere in the subject line. This will cause the email to be sent to the portal and the recipient will receive an email stating that they have a secure message.*

For assistance using the PharMerica Email Encryption Service, please contact PharMerica Technology Support at 877-581-6400 or email them at PharMericaSupport@PharMerica.com

Passwords:

- Choose passwords which are complex and which cannot be easily guessed (e.g., a unique password which makes sense to the Workforce member but not to anyone else), per PharMerica's policies.
- When creating a password do not use actual words (e.g., PharMerica, password), do not use your individual identifiers (names, driver's license number, social security number).
- Keep your user ids and passwords to access information systems containing PHI confidential and do not share

such information with anyone. If someone asks to use your password, report it to your supervisor.
- Do not post passwords or user IDs on or near your computer.
- If you share a workstation, only use your own password and logon ID to access data. Log-off when you are finished.
- Change your passwords as required by PharMerica's policies.
- If you suspect your password has been compromised or misused, immediately change the password, and report the incident to your supervisor and the HIPAA Security Officer**.**

Other Safeguards To Protect Electronic PHI:

- Remove PHI from training and presentation materials, including "screen shots" that display any patient information
- If you need to send PHI outside of PharMerica on a CD or jumpdrive, ensure that the CD/jumpdrive is encrypted (unless otherwise requested by a patient when requesting access to PHI).
- Lock your computers when stepping away from your computers and log off the computers at the end of the workday.
- Do not use personal e-mail (e.g., gmail, yahoo) to conduct PharMerica business.
- Do not e-mail any PHI to personal e-mail, text any PHI to personal cell phones, send any PHI via fax to any personal fax numbers (e.g., home fax number).
- Do not save, download or otherwise transfer any PHI on any personal computer, i-pad, hard drive, USB thumbdrive or other electronic device. Store PHI on PharMerica secured network servers.
- If you need to send PHI outside of PharMerica and sending such PHI via a secure e-mail is not practicable (e.g., due to large volume of documents), send the PHI via an upload to a secure document sharing site in coordination with the IT department, if feasible. If sending PHI via such methods is not feasible, PHI may only be sent via a personal delivery by courier or overnight delivery services with required recipient signature upon delivery (e.g., FedEx), and any electronic PHI sent via such method shall be via an encrypted disk or encrypted jump drive.
- Never disable or interfere with the virus protection installed in the workstations.
- Practice Safe Browsing Habits: stay current with browser updates and application updates such as Adobe Acrobat; enable browsing security settings to alert you to threats to your computer like popups, spyware, and malicious cookies.

Safeguard PHI on Mobile Devices

- Any mobile devices which may maintain, access or transmit PHI must be encrypted.
- You may use personally owned mobile devices only consistent with the requirements of PharMerica's policy on use of personally owned devices and only if the devices are encrypted via Mobile Iron or InTune. Coordinate all questions with IT Helpdesk.
- Personally owned electronic equipment cannot be connected to PharMerica's information system.
- Immediately report to the Security Officer and to the police a loss or theft of any mobile electronic device you use to access PharMerica's information system. Upon receiving such report, the Security Officer shall initiate immediate remote wiping of all data, including PHI, on that device, if technologically feasible.

Physical Security Safeguards

- Access to PharMerica facilities is physically restricted and requires a security badges scan for entry.
- Only PharMerica Workforce members, authorized contractors and authorized visitors may access PharMerica premises.
- Workforce members issued a security badge can only access the assigned areas.
- Safeguard access badges and any keys and do not share them with or borrow them to others.
- Make sure your security badges are visible at all times.
- Do not badge in other Workforce members. Each person must scan their own security badge, even if someone is holding the door.
- If you don't have a badge to enter PharMerica's facility in his or her possession, sign in as a visitor.
- If you lose a security badge, promptly contact the Facility Manager so a new security badge can be issued and the old security badge can be deactivated.

- All visitors must sign in at the front office, receive a security badge and be escorted by a Workforce member at all times while on PharMerica's premises.
- PharMerica premises are monitored by security cameras.

Restriction on Removal of PHI From PharMerica's Premises

Never remove any documents containing PHI outside of PharMerica premises unless required to perform their job responsibilities for PharMerica. If removal of PHI from PharMerica's premises is required to perform job responsibilities for PharMerica, remember:

- Electronic PHI shall be only on PharMerica issued devices and PHI shall be maintained in such devices in encrypted form.
- Any PHI shall be limited to the minimum necessary amount to perform the work needed, appropriately safeguarded at all times while off PharMerica's premises and returned to PharMerica premises as soon as practicable.
- The documents and devices containing PHI shall be at all times safeguarded. For example, do not check in as baggage when travelling, do not leave unattended in a car, do not leave unsecured at home, hotel or other location.

Important: Each Workforce member must carefully review PharMerica Policy #2 Safeguards to Protect the Privacy of Protected Health Information and utilize such safeguards in their daily job functions. You must also follow all other safeguards with respect to electronic PHI set forth in PharMerica's security policies.

BREACH OF UNSECURED PHI REQUIREMENTS

What is a Breach of Unsecured PHI?

Under the HIPAA Breach Notification Regulations PharMerica must notify affected patients, OCR and in some cases, media, in the event of a Breach of patients' Unsecured PHI. Electronic PHI is considered Unsecured PHI if the PHI is not encrypted. Paper PHI is Unsecured PHI unless paper records have been shredded. Breach is the acquisition, access, use of disclosure of PHI in a manner not permitted by the Privacy Regulations that compromises the security or privacy of the PHI. Examples of incidents that can constitute a Breach:

- A prescription is sent to the wrong recipient
- Paper records with PHI were thrown into trash
- Electronic device containing PHI is lost
- Unauthorized party gains access to a server
- Documents with PHI are lost
- PHI is sent to a personal e-mail account

The list above are just examples and not an exhaustive list of incidents that could constitute a Breach. If you re in doubt whether a particular event is an incident that needs to be reported to the Privacy Officer, please contact the Privacy Officer for guidance and direction.

Reporting Requirement for PharMerica Workforce Members

All PharMerica Workforce members must report to the Privacy Officer all actual or suspected incidents of use or disclosure of PHI believed to be in violation of the Privacy Regulations of which they become aware. If **you know or suspect that an impermissible use or disclosure of PHI has occurred, immediately notify the Privacy Officer.** To report a potential incident, complete, in coordination with your pharmacy's Privacy Coordinator, an *Unsecured PHI Incident Report* and send to privacy.department@pharmerica.com for evaluation and risk assessment. If you become aware of an incident of impermissible use or disclosure of PHI by a PharMerica's business associate, also report this information immediately to the Privacy Officer in the same manner.

Investigation and Notification Requirements

The Privacy Officer will review all reported incidents, perform a risk assessment to determine if a Breach of Unsecured PHI has occurred and take prompt mitigation steps. The appropriate mitigation steps will vary depending

on the nature of the Incident and will be determined by the Privacy Officer on a case by case basis. If an incident is determined to constitute a Breach of Unsecured PHI, PharMerica will notify of the Breach:

- Each patient whose Unsecured PHI has been, or is reasonably believed to have been, Breached without unreasonable delay and no later than 60 days after PharMerica discovered the Breach;
- The Secretary of the U.S. Department of Health and Human Services ("HHS"); and
- Prominent media outlets serving the state or jurisdiction if the Breach involves more than 500 residents of such state or jurisdiction.

If Breach involved a covered entity customer of PharMerica and impacted PharMerica in its role as a business associate, Privacy Officer will coordinate appropriate notification to such customer.

Important: Please review PharMerica's Privacy Policy #22, Notification for Breach of Unsecured PHI, which addresses compliance with the breach notification requirements.

BUSINESS ASSOCIATES

PharMerica's Business Associates

A vendor who performs services for or on behalf of PharMerica that involve the creation, receipt, maintenance, or transmission PHI is considered a business associate of PharMerica. Examples of vendors which may be considered business associates of PharMerica include:

- E-prescribing gateway
- Vendors providing data storage services
- Information technology vendor maintaining PharMerica's computer and networks system
- Vendor providing document shredding service
- Consultants
- Billing company
- Collection agency

The above list provides just examples and is not an exhaustive list of the types of service providers that may be considered business associates of PharMerica. If you need guidance regarding the need for a Business Associate Agreement with a particular vendor, contact the Privacy Officer who will provide clarification and direction.

Business Associate Agreements With PharMerica's Business Associates

Before any PHI may be shared with a business associate, PharMerica must require the business associate to safeguard PHI. This is done through a written business associate agreement ("BAA") with the business associate. The BAA contractually binds the business associates to comply with the applicable requirements of the Privacy Regulations, with the Security Regulations and Breach Notification Regulations. Business associates, in turn, must then contractually bind any of their subcontractors to whom they provide PHI when performing services to PharMerica to these same requirements.

What Does This Mean To You?

Before engaging any vendor that will need access to PharMerica's PHI, the Workforce member engaging the vendor must request that the vendor enter into a BAA with PharMerica. **No Workforce member may permit any vendor to access, use, disclose, maintain or transmit PHI for or on behalf of PharMerica unless there is a BAA with the vendor.**

- Contact the Privacy Officer at privacy.department@pharmerica.com if you need to enter into a BAA. PharMerica has adopted a form BAA to use with PharMerica's business associates. ***Form #18A in the Privacy Manual, Form Business Associate Agreement – PharMerica is a Covered, is PharMerica's approved BAA.***
- If the vendor requests changes to PharMerica's form BAA or requests that another BAA be used, contact the Privacy Officer for review and approval.
- The BAA may be executed on behalf of PharMerica only by the heads of business units holding Vice President or above title or by the Privacy Officer.

- If you become aware of any known or suspected breach of a BAA, immediately report this information to the Privacy Officer who will investigate the matter and coordinate appropriate steps.

PharMerica As a Business Associate of Other Covered Entities

PharMerica may also be a business associate to other covered entities if PharMerica is providing services to those covered entities that requires access to PHI. For example, PharMerica may be business associate of a long term care facility when it performs consulting or administrative services to such facility. If PharMerica is providing services to another covered entity and will need access to that covered entity's PHI, PharMerica must enter into a BAA with that covered entity. In connection with providing services to with respect to which PharMerica is a business associate, PharMerica shall use and disclose PHI only as permitted or required by the terms of the applicable BAA.

What Does This Mean To You?

- Contact the Privacy Officer at privacy.department@pharmerica.com and the contracting department at contracting@pharmerica.com if PharMerica must enter into a BAA with another covered entity. PharMerica has adopted a form BAA to use with covered entities for whom PharMerica is a business associate. ***Form #18B in the Privacy Manual, Business Associate Agreement – PharMerica is a Business Associate, is PharMerica's approved BAA.***
- If the covered entity customer of PharMerica requests changes to the form BAA or requests that another BAA be used, contact the Privacy Officer for review and approval.
- The BAA may be executed on behalf of PharMerica only by the heads of business units holding Vice President or above title or by the Privacy Officer.

Who Has a Copy of PharMerica's BAAs?

Privacy Officer maintains all Business Associate Agreements to which PharMerica is a party. If you have a question about an existing BAA, please contact the Privacy Officer.

Important: Please review PharMerica Policy #18, Disclosure of Protected Health Information to Business Associates, which addresses requirements for entering into business associate agreements. You must also review Forms 18A and 18B and be familiar with the requirements of the BAAs.

PATIENT PRIVACY RIGHTS

Right to Access PHI

Patients have the right to inspect and receive a copy of their pharmacy and billing records maintained by PharMerica. Patients have this right for as long as the PHI is maintained by PharMerica regardless of the date the PHI was created, whether we maintain such PHI in paper or electronic form, whether the PHI is maintained onsite or in an offsite storage or where the PHI originated (e.g., PharMerica, another provider). Patients also have the right to direct PharMerica to provide their PHI directly to another entity or person designated by the patient. Patients do not need to tell us why they would like to receive a copy of their PHI. Requests to access PHI must be submitted to PharMerica in writing. A patient may use **Form 9A, Request to Access PHI** to submit such request. PharMerica must review and respond to each request as soon as possible and no later than 30 calendar days after the receipt of the request. If a state law requires to respond sooner, we must comply with the state law required shorter timeframe. PharMerica will provide the patient with access to the patient's PHI in the form and format requested by the patient, if it is readily producible in such form and format; or, if not, in other format agreed with the patient. There are limited grounds that may permit denial of a patient's request to access their PHI. Fees for providing a patient with a copy of the PHI are strictly regulated by the Privacy Regulations and PharMerica may only charge a reasonable, cost-based fee for providing copies of PHI to the patient.

If your pharmacy receives a request for PHI, please notify your pharmacy's Privacy Coordinator who will submit the request to the Privacy Officer for review and response by sending a copy of the request to privacy.department@pharmerica.com. The Privacy Officer will review each request and coordinate with the Privacy Coordinator the timely response to the request.

Important: Please review PharMerica Policy # 9, Patient's Right of Access to Protected Health Information, which addresses PharMerica's process for handling patients' request for access to their PHI.

Right to Amend PHI

Patients have the right to request amendment of their PHI if they believe that the PHI we keep about them in the pharmacy or billing records is incorrect. Any requests for an amendment must be in writing, directed to the Privacy Officer and provide a reason to support a requested amendment. ***Form #11A in the Privacy Manual, Request for Amendment of PHI*** may be used for such request. The Privacy Officer will review and coordinate a response to each request. If PharMerica agrees to make a requested amendment, PharMerica will make the amendment, notify the patient that the amendment was made and notify others as directed by patient about the amendment. PharMerica may deny the patient's request for amendment in certain situations, such as if the PHI being amended was not created by us, if we believe the PHI is already accurate and complete, or if the PHI is not contained in records that the patient would be permitted to access. If the request for amendment is denied, PharMerica must inform the patient as required by the Privacy Regulations.

If your pharmacy receives a request for PHI amendment, please submit the request to the Privacy Officer for review and response by sending a copy of the request to privacy.department@pharmerica.com. The Privacy Officer will review each request and coordinate the response to the request.

Important: Please review PharMerica Policy # 11, Patient's Right to Request Amendment of Protected Health Information, which addresses PharMerica's process for handling patients' request to amend their PHI.

Right to Select How to Receive Communications of PHI

Patients have a right to request that PharMerica communicates with them using a specific communication method or at a specific location. For example, a patient may ask that we call them only at a specific phone number or send communications to a specific mailing address. If your pharmacy receives a patient request that any communications from PharMerica to the patient be made using a specific communication method or at a specific location, instruct the patient to complete ***Form #12 in the Privacy Policies, Request for Confidential Communication of PHI.*** If your pharmacy receives a completed Form #12, please submit the completed form to the Privacy Officer at privacy.department@pharmerica.com. Patients should not be ask about the reason for their request. PharMerica will accommodate reasonable patient requests for confidential communications. The Privacy Officer will review the request and determine if it is administratively feasible for PharMerica to accommodate the request. If PharMerica will agree to the request, all appropriate individuals responsible for communicating with the patient (e.g., pharmacy personnel, billing personnel) will be informed of the request.

Important: Please review PharMerica Policy #12, Patient's Right to Request Confidential Communication of Protected Health Information, which addresses PharMerica's process for handling patients' request for confidential communications of their PHI.

Right to Request Restrictions On Certain Uses and Disclosures

Patients have the right to request restrictions on PharMerica's uses and disclosures of their PHI for treatment, payment or healthcare operations or to individuals involved in their care. PharMerica is not required to agree to a patient's request unless the patient requests PharMerica to restrict disclosure of PHI to a health plan and (a) the disclosure is for carrying out payment or healthcare operations (and not for the purpose of carrying out treatment), (b) the PHI pertains to the items or services for which the patient (or person other than the health plan on behalf of the patient) paid out-of-pocket in full, and (c) the disclosure is not otherwise required by law. 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 tell the patient that we do not accept the restriction.

If your pharmacy receives a patient request for restrictions on PHI disclosures, instruct the patient to complete ***Form #13 in the Privacy Policies, Requests for Restriction on Use and Disclosure of PHI***. If your pharmacy receives a completed Form #13, please submit the completed form to the Privacy Officer at privacy.department@pharmerica.com.

Important: Please review PharMerica Policy # 13, Patient's Right to Request Restrictions on Use and Disclosure of Protected Health Information, which addresses PharMerica's process for considering and responding to patients' request for restrictions on the use or disclosure of their PHI.

Right to Obtain an Accounting of PHI Disclosures

Patients have a right to request a report of the disclosures of their PHI by PharMerica. A patient may ask for an accounting of PHI disclosures that were made during the six years prior to the date of the patient's request. We are not required to give the patient an accounting of the disclosures that we have made for purposes of treatment, payment, or healthcare operations, or for certain other disclosures, such as disclosures for which we received written patient's Authorization. Examples of disclosures that PharMerica must account for when responding to a patient's request for an accounting are disclosures to attorneys or courts for litigation (unless the patient provided Authorization for that disclosures), disclosures to health oversight agencies (e.g., DEA, CMS, state Board of Pharmacy), disclosures to law enforcement. PharMerica must provide one accounting to each patient in any 12-month period without charge and any additional requests in the same 12 month period may be subject to certain limited charges. Patients need to submit a request for accounting in writing directed to the Privacy Officer. **Form #10(A) in the Privacy Manual, Request for Accounting of Disclosures of PHI** may be used.

If your pharmacy receives a request for accounting from a patient, please forward the request to the Privacy Officer at privacy.department@pharmerica.com. The Privacy Officer will review each request and coordinate the timely response to the request.

Important: Please review PharMerica Policy # 10, Patient's Right to Accounting of Disclosures of Protected Health Information, which addresses PharMerica's process for handling patients' request for an accounting of disclosures of their PHI.

Right to File a Complaint

Patients have the right complain about PharMerica's privacy policies and procedures, compliance by PharMerica with its privacy policies and procedures, or compliance by PharMerica or our business associates with the Privacy Regulations. Patients may complain to PharMerica or to the HHS. Patients may submit complaints in writing or verbally. *Form #15 in Privacy Policies, Complaints Regarding Privacy Policies and Procedures* may be used to submit the complaints to PharMerica. If your pharmacy receives a complaint from a patient, please promptly forward the complaint to the Privacy Officer at privacy.department@pharmerica.com. The Privacy Officer will review each complaint and coordinate an appropriate response to the complaint. PharMerica does not retaliate against any patient or the patient's personal representative for filing complaints.

Important: Please review PharMerica Policy #15, Complaints Regarding Privacy Policies and Procedures, which addresses PharMerica's process for handling patient complaints.

SANCTIONS FOR NONCOMPLIANCE WITH HIPAA AND PRIVACY POLICIES

PharMerica Workforce members are required to complete HIPAA privacy training, understand the Privacy Policies and comply with the Privacy Policies and Privacy Regulations. If you know or reasonably suspect a use or disclosure of PHI in violation of the Privacy Policies you must report the violation to the Privacy Officer. If a Workforce member is found to violate the Privacy Policies, such individual will be subject to appropriate sanctions. The sanctions can range from warning to termination of employment with PharMerica.

Important: Anyone found violating privacy of PharMerica's patients may be disciplined per HIPAA Sanctions Policy. Please review PharMerica Policy # 17, Sanctions for Failure to Comply with Privacy Policies and Procedures.

ADDITIONAL LEGAL AND COMPLIANCE REQUIREMENTS

Privacy Regulations preempt state laws that are contrary to the Privacy Regulations. The basic tenets of this rule are that if a state law is less strict than the Privacy Regulations then the Privacy Regulations control. If a state law is stricter than the Privacy Regulations or provides patients with more rights than the Privacy Regulations, then both the Privacy Regulations and state laws apply. It is also important to remember and always comply with many other Federal and state laws govern our operations. For example, our pharmacies must comply with the DEA requirements, state Board of Pharmacy regulations, Federal laws on protection of alcohol and drug abuse records and state medical record confidentiality laws. Many Workforce members are healthcare professionals bound by the ethics rules of their professions and they must always stay within the bounds of those rules. In addition, importantly, all Workforce members, regardless of function or position, are required to comply with all PharMerica's policies and procedures and PharMerica's *Code of Business Conduct and Ethics*.

For additional HIPAA compliance resources, please visit the Privacy and HIPAA Compliance site.
For any questions about HIPAA compliance or Privacy Policies, please contact the Privacy Officer.