HIPAA Privacy and Procedure Policy
Pulmonary Medicine Associates

Effective 01/01/2012
Revised 10/30/2019
Version# 19.1

Table of Contents

Overview

In 1996, the federal government enacted the Health Insurance Portability and Accountability Act ("HIPAA"), in response to the increasing concern about patient privacy and confidentiality during a time of increased demand for access to medical information by providers and other entities. The Department of Health and Human Services ("DHHS") drafted both security and privacy regulations, as well as introduced the Health Information Technology for Economic and Clinical Health Act ("HITECH").

The Privacy Rule is more focused on patient and client rights to control the uses and disclosures of all Protected Health Information (PHI) while the Security Rule specifies how covered entities must protect electronic PHI ("ePHI").

The HITECH Act facilitates the expansion of the Electronic Medical Record (EMR) standards that aid in electronic exchange of health information on a national basis to make medical care more organized and transparent. The HITECH Act is committed to the cause of seeing that healthcare entities adopting EHR methodologies do so within the realm of the HIPAA Privacy Rule and Security regulations.

In order to strengthen the privacy and security protections for health information established under HIPAA, the Final Omnibus Rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law.

Purpose

The purpose of this policy is to provide guidance to the employees of Pulmonary Medicine Associates (PMA), by setting forth the basic requirements for protecting the confidentiality of protected health information as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, particularly the Security Rule and the Privacy Rule. This policy will be reviewed and/or updated no less than once per year.

Policy Statement

The following security and privacy policies have been adopted to ensure that PMA complies fully with all federal and state privacy protection laws and regulations. Protection of patient privacy is of supreme importance to this organization. Violations of any of these procedures and policies may result in disciplinary action, up to and including termination of employment, and possible referral for criminal prosecution. PMA is committed to maintaining reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and confidentiality of health care information.

Sanctions

Violations of this policy may result in disciplinary action up to and including termination of employment. Please refer to the disciplinary procedure in your employee handbook.

Contact

Chief Privacy Officer: **Amit Karmakar, M.D.**
5 Medical Plaza Drive, Suite 190
Roseville, CA 95661
Phone (916) 786-7498 | Fax (916) 786-2715
akarmakar@pmamed.com

Definitions

1. "**Patient**" means any person who has registered and has received services at PMA without regard to date of services

2. "**Protected Health Information**" ("PHI") means individually identifiable health information, including demographic information collected from an individual, in any form, created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, and future physical or mental health or condition of an individual; the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

3. "**Violation**" occurs when an employee fails to comply with a federal or California law or regulation, or a policy of PMA regarding the protection of PHI.

4. "**Workforce**" means employees, volunteers, trainees, and other persons under the direct control of PMA, whether or not paid by PMA. Workforce also means any independent contractors who interact with PHI and who have not signed a Business Associate Agreement.

5. "**Workstation**" means the principle point of contact when accessing electronic information within PMA. The reference to Workstation includes fully functional Desktop PCs, Diskless Terminals, Laptops and other portable devices such as notebooks, smart phones, and PDA's.

If you have any questions about the information in this Policy or any HIPAA regulations, please ask your immediate supervisor.

Policy Section

HIPAA Privacy and Procedure Policy

Notice of Privacy Practices (NOPP)

Implemented: March 2012

Last Updated: August 2017

Purpose: To provide guidance in understanding PMA's Notice of Privacy Practices (NOPP)

HIPAA Notice of Privacy Practices (NOPP) document informs patients how PMA may use and share their health information and how they can exercise their health privacy rights. The NOPP also includes an agreement to the arrangement by which a patient requests that their health benefit payments be made directly to PMA. Downloading a patient's medical record, including medication and vaccine histories, via interface, are also covered. It is PMA's policy to offer patients a copy of the NOPP at each visit at the time of check-in.

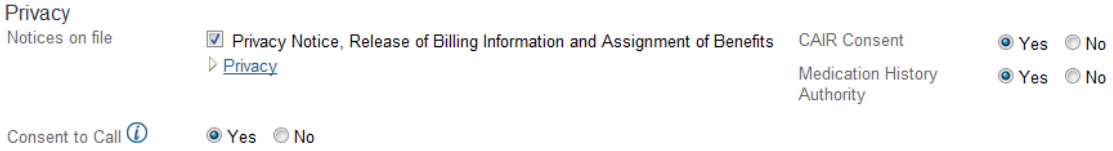
This notice is provided to the patient with their New Patient Information Packet, on the Patient Portal under the "medical forms" section and on PMA's website. Additionally, a copy of the NOPP must always be made available to our patients in the reception area.

It is not mandatory that a patient sign an acknowledgement of receipt of the NOPP in order to be seen by a provider in the practice, however, it is required that PMA provide the patient a copy of the notice. In situations where the NOPP is given to the patient and patient declines to sign, staff should make a notation on the signature page of the registration form and upload to the patient's chart.

Proper Documentation of HIPAA Notice of Privacy Practices Form, Assignment of Benefits, Medication History Authority and Consent to Call in athena

It is only permissible for staff to check the appropriate boxes within the Quickview screen at the time of check in, after the patient has acknowledged receipt for or been provided the *HIPAA Notice of Privacy Practices* form.

Note: We must get verbal consent from the patient to receive automated calls to their cellular phone as this is not covered by HIPAA law. Yes for the "consent to call" option should only be chosen if the patient gives verbal consent to receive automated calls directly to their mobile phone.



Covered Entities

A covered entity includes those individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA. They must comply with HIPAA rules and requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. Examples of entities include health care providers, health plans and healthcare clearinghouses.

The following is a sample list of entities for which additional consent from patients is not necessary prior to disclosing protected health information:

- Primary Care Physicians or Primary Treating Physicians
- Referring Physicians
- Any entity that a PMA provider refers the patient to
- Insurance Companies
- Insurance Adjusters
- Any third party entity that either has or had a relationship with the individual who is the subject of the information, and the protected health information pertains to the relationship
- As required by law for the following: Public Health Issues and Communicable Diseases; Health Oversight such as Abuse or Neglect; Food and Drug Administration requirements; Legal proceedings; Law Enforcement; Coroners; Funeral Directors and Organ Donations; Research; Criminal Activity; Military Activity and National Security; Worker's Compensation; Inmates

Additionally, patients are given the opportunity to add an Emergency Contact to their new patient registration sheet. It is important that only the person listed by the patient be added to the Emergency Contact fields in athena. The patient must consent to the following clause that relates to telephone/in office communication:

> *In addition to being my emergency contact, I authorize PMA to communicate with the individual listed below regarding any medical and/or financial issues.*

Patients must notify PMA in writing if they wish us to restrict, disclose or obtain any information from any person or entity that does not fall under the authorization of the NOPP document. This includes authorizations or restrictions for family members and friends. See Policy for Release of Medical Records for more information.

HIPAA Privacy and Procedure Policy

Release of Medical Records Policy

Implemented: March 2012

Last Updated: December 2016

Purpose: To ensure workforce understanding of procedures regarding the release of patients' Protected Health Information (PHI)

If a representative from any government agency comes to the office and requests the release of any PHI, immediately notify your supervisor and PMA's Privacy Officer.

For all consented disclosures, please have patients fill out the PMA Authorization to Release Medical Records Form.

In order for the PMA signed Authorization for Use or Disclosure form to be valid, all of the following information **must** be filled out by the patient:

- Purpose for release;
- Specific information being requested;
- Dates of records requested; and
- Specific permission for special consent (if applicable)

Release of electronic or paper requests for copies of medical records of PMA Clinic Patients

All HIPAA-covered entities using electronic health records are required to honor a patient's request for an electronic copy of her/his medical record, which must be transmitted directly to an entity or person specified by the patient, as long as that directive is clear, conspicuous, and specific. HIPAA requires that such requests be honored within 3 days of the request for electronic records and 30 days for paper records. PMA provides electronic medical record copies via password encrypted CD-ROM.

PHI can be mailed out or sent through fax to any entity that has a responsibility to protect patient privacy as documented by HIPAA law. With written authorization from the patient, paper records containing less than 25 pages may be mailed to them.

Due to the time sensitivity of disclosure requests, clinic staff is asked to upload any signed authorization forms to the patient's chart for medical records to address promptly. Clinic staff should also collect any fees associated with the release for quicker turnaround.

Please note: All information stored in the patient's chart, whether or not it was created by PMA, must be released if requested by the patient.

It is permissible to publish lab/imaging results directly to the patient's portal without a patient's written consent. If the patient is in the office and asks for a printed copy of one test result, that can be released without written consent as well. Although it is preferable to publish these to the patient's portal, we can provide a paper copy if preferred by the patient. This must be done through chart export so that the disclosure is documented correctly in athena. Any time a patient requests more information than can be published to the portal or any more than 2 items, the patient must sign a release of records and their record request will be processed by medical record staff.

In order to release physical copies of medical records or encrypted CD-ROM to the patient or other authorized persons, it is PMA's policy to have at least one of the following:

- Release of Medical Records Request form completed and signed by the patient OR
- Faxed request by another covered entity requesting medical records which includes their letterhead, dates of records requested and a business reason for the records, OR
- Signed subpoena or court order requesting the documents

All signed correspondence will be uploaded to the patient's athena chart under the classification "Admin-Medical Records Request". The chart export function in athena must always be used to fax or print out the requested documents so that proper, accurate documentation of what is being disclosed is recorded in the medical record.

Paper Record Transfers To Clinics

For inter-office transfers within PMA, any correspondence containing protected health information must be sent through the courier service. PMA does not permit staff to take (hand-carry) correspondence containing PHI outside of the current PMA office.

Release of electronic or paper requests for copies of medical records of Hospital Patients consulted by PMA Providers

When a patient is seen only in the hospital or has had a test interpretation by a PMA provider in the hospital setting, they must be referred to the rendering facility to obtain those records.

If a patient sends us a written authorization for a release of information, we must fulfill that request if we have such records on file. However, it is PMA's policy to assist and encourage the patient to request records through the rendering facility itself.

Release of medical records for Deceased Patients

PMA may release medical information to coroners, medical examiners and funeral directors as necessary to carry out their duties and as required by law. It is not permissible to release any medical information to any other entity or person without a signed subpoena, court order, or other official document permitting such release.

All HIPAA release forms and the powers they grant expire upon the patient's death. The rights conveyed by a Medical Power of Attorney expire upon the patient's death, as well. Only the patient's designated "personal representative" has a right under law to access the deceased person's medical record. The law does not give any other person the right to obtain access to a deceased patient's records.

California defines a "personal representative" as the beneficiary or personal representative of the deceased patient. Therefore, a deceased patient's beneficiary or personal representative will have the same right of access as the patient would have had if he or she were still living. The beneficiary is anyone who will inherit from the patient by will or estate. The personal representative is either the administrator or the person's legal executor under the patient's will. Legal documentation must be provided to prove one is the "personal representative" of a deceased patient. A combination of the death certificate, court document establishing estate executorship, and a signed release of medical records is sufficient to establish one's right.

New HIPAA regulations permit PHI to be communicated to persons or entities that would have been covered if the patient were living. Communication related to treatment, payment, or health care operations, are permitted so as long as the patient did not restrict prior to death. This does not apply to the release of physical paper or electronic records.

Disclosures Requiring Special Consent

In order for PMA to disclose Highly Confidential Information for purposes not related to treatment, payment, or health care operations, we must obtain a patient's separate and specific written consent. Highly confidential information includes Drug and/or Alcohol Dependency, Sexually Transmitted Diseases, AIDS/HIV and Psychiatric (Mental Health) Records. PMA's Authorization to Release Medical Records Form includes a section for these types of disclosures.

Documenting Authorizations to Obtain and Disclose Health Information in Athena

The individual listed by the patient on their registration form in regards to their emergency contact will be recorded in the full registration page in Athena. This form will be uploaded into the patient chart and properly labeled for reference.

All signed Authorization forms to obtain and disclose health information must be uploaded into the patient chart and labeled accordingly. For disclosures to medical professionals and entities, this information will be added to the "Patient Care Team" section of the health history tab.

Patient Right to Inspect and Copy

A patient has the right to inspect and copy their medical record information, and that usually includes medical and billing records. The patient must submit their request in writing to the PMA Medical Records Department.

This request may be denied if the patient is requesting mental health notes or any information compiled in anticipation of use in a civil, criminal or administrative action or proceeding. If any patient's chart contains any of these documents, these requests are to be forwarded to the usual provider for approval or to the Privacy Officer in the event the usual provider is no longer with PMA.

If denied, the patient may request the denial be reviewed and PMA will choose another licensed health care professional to proceed with the review. All patient requests for their denial to be reviewed will be forwarded to the Privacy Officer.

Patient's Right to Amend

If a patient believes that the information included in their medical record is incorrect or incomplete, they may ask us to amend the information. This request must be made in writing and be submitted to the PMA Medical Records Department. A supporting reason must accompany the written request. Requests may be denied if:

- The request is not in writing or does not include a reason to support the request;
- The information was not created by PMA, unless the person or entity that created the information is no longer available to make the amendment;
- The information is not part of the medical record kept by or for PMA;
- The information is not part of the record in which you were permitted to inspect and copy; or
- The information is accurate and complete

These requests are to be forwarded to the usual provider for review or to the Privacy Officer in the event the usual provider is no longer with PMA.

In the event the request is denied, a patient may still submit a written addendum which does not exceed 250 words, with respect to any item or statement in their record they believe is incomplete or incorrect. This document may be attached to the patient's chart if requested, and will be included whenever PMA makes a disclosure of the original item or statement referenced in the patient's addendum.

Patient Rights to an Accounting of Disclosures

A patient has a right to request an "accounting of disclosures". The accounting of disclosures is a list of all of the disclosures of PHI that PMA has made regarding the patient. The list can be found under the privacy information in the patient's clinical chart.

The patient must submit their request for the disclosures in writing to the PMA Medical Records Department. The request must state the time period and in what form they want the list (paper or electronic). This disclosure must also be noted in the accounting of disclosure notes within athena.

Patient Rights to Request Restrictions

A patient has a right to request a restriction or limitation of the medical information PMA uses or discloses for treatment, payment or health care operations. A patient can also request a restriction or limitation for a specific person who is directly involved in the care or payment, such as a family member or friend.

A patient has the right to restrict PMA from disclosing PHI from their health plan as long as they are paying for their care in full out of pocket, and has requested such restriction in writing.

The patient must submit their request in writing to the PMA Medical Records Department. The request must include the following:

- What information the patient wants to limit
- Whether this is to limit the use and/or disclosure of that information
- To whom the limits apply

PMA is not required to comply with the request, and such requests must be forwarded to the usual provider for approval or to the Privacy Officer.

Patient Rights to Confidential Communications

A patient has the right to request that we communicate with them about medical matters in a certain way or at a certain location. For example, a patient can ask that we only contact them at work or by mail.

The patient must submit their request in writing to the PMA Medical Records Department. The request must specify how or where the patient wishes to be contacted. This information will be added to the "Confidential Communications" section in the patient's clinical chart.

Patient Rights to a Paper Copy of the Notice of Privacy of Practices (NOPP)

It is PMA's policy to offer patients a paper copy of the NOPP at each visit at the time of check in. This form can also be found on the patient portal and on the PMA website. The patient has a right to a paper copy of this notice, even if they have agreed to an electronic version**.** Additionally, PMA will have laminated copies of the most current NOPP available to patients in the reception area.

Complaints to PMA

All complaints from a patient related to their privacy rights must be forwarded immediately to the Privacy Officer.

Fees

All requests for medical records should be accompanied by a 15.00 copy fee.

HIPAA Privacy and Procedure Policy

Unauthorized Access of Medical Records Policy

Implemented: March 2012

Last Updated: November 2015

Purpose: To ensure that workforce members refrain from using PMA-authorization to access their own personal medical records

All covered entities, including Sutter, Mercy, and PMA are required to have procedures in place that both prevent unauthorized access to medical records and permit patients access to their own medical records. As a Business Associate, PMA is obligated to prevent unauthorized access to the Protected Health Information of our fellow HIPAA-covered entities, including but not limited to, Sutter, Mercy, imaging and lab vendors.

- PMA workforce members may only access files or programs, whether computerized or otherwise, that are necessary to perform their job functions. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems, or programs, or other property of PMA or improper use of information obtained by unauthorized means, may be grounds for disciplinary action up to and including termination of employment.

- Workforce members may not, under any circumstances, use a PMA computer or other PMA equipment, or a PMA assigned user ID and/or password and/or token to access their own personal or any other medical record unless there is a PMA business purpose to do so.

- On non-work time, such as breaks or meal periods, workforce members may use PMA computers to access their own or a family member's (if authorized) Protected Health Information if using their own personal patient-authorized means such as a patient portal or medical group Web site with an appropriate patient-specific user name and password.

HIPAA Privacy and Procedure Policy

Minimum Necessary Policy

Implemented: March 2012

Last Updated: March 2012

Purpose: To limit the disclosure or acquisition of PHI to the minimum necessary for business purposes

Minimum Necessary Policy

When using or disclosing Protected Health Information (PHI), or when requesting PHI, PMA workforce will make reasonable efforts to limit the PHI used, disclosed, or requested, to the minimum necessary.

Protected Health Information is defined as individually identifiable health information, including demographic data that relates to:

- The patient's past, present, or future physical health or condition
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual

PHI is more than just the medical record. PHI also includes financial, demographic, and lifestyle information. This includes paper, electronic and spoken information.

The minimum necessary standard is a key protection of the HIPAA Privacy Rule. Minimum necessary means that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a specific function.

This policy is **not** intended in any way to impede access to patient information necessary for healthcare providers to make medical decisions and provide treatment to the patient whose information is requested or disclosed.

Exclusions: The minimum necessary requirement does **not** apply to any of the following:

- Disclosures to or requests by a health care provider for treatment purposes;
- Uses or disclosures made to the individual who is the subject of the information;
- Uses or disclosures made pursuant to a valid and HIPAA-compliant authorization signed by the patient or patient's Legal Representative;
- Disclosures made to the United States Department of Health and Human Services, or any officer or employee of that Department to whom the authority involved has been delegated;
- Uses or disclosures Required by Law; and
- Uses or disclosures required for compliance with other applicable laws and regulations.

PMA will identify which job classifications need access to what type of PHI to carry out their job responsibilities.

Need to Know Principle

PMA workforce members are not permitted to access the PHI of a patient unless there is business reason for doing so.

PMA workforce members may not discuss or disclose any PHI to someone who does not need to know the information.

PMA workforce members should not have discussions about patients with other PMA staff who do not have a need to know.

HIPAA Privacy and Procedure Policy

Telephone and Office Privacy Policy

Implemented: March 2012

Last Updated: March 2014

Purpose: To provide guidance for appropriate PHI communication by telephone and in the office environment

Telephone Privacy Procedures:

All Staff are permitted to communicate the following information to a patient by phone. Messages may be left on a voice answering device or with a physical person, indicating the following:

- Employee must state name, title and that you are calling from "Pulmonary Medicine Associates" with your contact information
- Appointment Confirmation/Reminders
- A message to have the patient call the office
- Clinic Address for the patient's appointment

Front Office / Central Scheduling staff may further discuss with the patient OR the person listed by the patient as their emergency contact OR any individual that the patient has given a verbal or written consent to disclose medical/financial information:

- Verification of correct patient demographics
- Verification of insurance/guarantor information
- Patient Portal registration and login instruction
- Collection of demographic/financial information, primary and referring physician information, patient preference for pharmacy/lab and any other need to know information to complete patient registration processes
- Co-pay or co-insurance information
- Insurance Referrals, Authorizations and Denials

Check-out staff may further discuss any information needed from the patient to complete outgoing orders to referred entities. This may include:

- Preference to time/date for scheduling procedures
- Preference to location where services are to be performed

Medical Records Staff may further discuss the following with the patient OR the person listed by the patient as their emergency contact OR any individual that the patient has given a written consent to disclose medical/financial information:

- Dates of office visits or other in-house procedures
- Availability of Records
- Passwords to open encrypted CD's created through athena

Please note that all billing inquiries must be directed to the billing staff at the Business Office.

Billing Staff are permitted to communicate the following information to a patient by phone. Messages may be left on a voice answering device or with a physical person, indicating the following:

- Employee must state name, title and that you are calling from "Pulmonary Medicine Associates" with your contact information
- A message to have the patient call the office

Billing Staff may discuss the following with the patient OR the person listed by the patient as their emergency contact OR any individual that the patient has given a written consent to disclose medical/financial information:

- Dates/locations of services rendered
- Financial and demographic information, including health plan information, primary and referring physician information, or any other need to know information to complete proper billing procedures
- Balance due and current status of account

If the nature of the call is in regard to hospital billing, billing staff may speak to any individual to collect any information necessary to complete their job solely for billing purposes. This is permitted under HIPAA law if the person is agreeable to release such information and as long as no other PHI regarding specific treatment is disclosed. Proper documentation of the call must be recorded in the patient's account.

Medical Assistants are allowed to communicate the following with the patient OR the person listed by the patient as their emergency contact OR any individual that the patient has given a written consent to disclose medical/financial information:

- Normal lab or "abnormal - as expected" results as approved by a provider
- Transmit information as instructed by the provider
- Collect any PHI or message to convey to a provider as a patient case
- All telephone conversations where health information is discussed (appointment scheduling not included) must be documented in the electronic medical record

A Medical Assistant should NEVER provide a diagnosis, medical advice, or any abnormal lab or imaging result unless instructed by provider documentation. It is permissible to say on a voicemail that recent tests were normal, but not say what testing was done. Invite the patient to call the office if they would like more information.

Verbal Consents

In situations where a patient verbally asks the PMA employee to talk to or call another person on their behalf, it is permissible as long as it remains limited to that call and must be completed by the same PMA employee. In addition, this must fully be documented in the document action notes or other acceptable field in athena, with the inclusion of the patient's verbal consent details.

Office Privacy Procedures:

Discussion of PHI, between patient, providers and staff must be kept to a minimal voice level, particularly in common areas such as the front desk and lobby. Discussion of patients and their PHI is forbidden in the break room.

Yelling at or calling for someone from a distance is not permissible. Staff should either walk to the person so that discussion can be private or the phone should be utilized.

When on the phone, voice should be kept at the lowest level possible. In circumstances where a patient, or other party, may be hard of hearing, it is advisable to ask if they may be placed on hold while the staff changes phones in a more private area where a raised voice may be used.

When calling a patient from the lobby for their exam, patients must be addressed by the appropriate title (Ms. Mrs., Miss, Mr., Dr.,) and last name. There is no exception. In circumstances when there are two or more people who are checked in with the same last name, it is permissible to add the first name as well. Once the patient has left the lobby area, it is acceptable to address a patient by another name, such as their first name or a nickname, if invited to do so.

HIPAA Privacy and Procedure Policy

Workstation Use Policy

Implemented: March 2012

Last Updated: March 2012

Purpose: To provide guidance regarding the proper safeguarding of workstations to prevent unauthorized use and to protect PHI

Desks

All employees shall be assigned log-on credentials by the IT department to use their workstation computers.

Computer Screens should never be visible to patients or other unauthorized individuals. In circumstances where computer screens must face patient areas, a security screen or privacy shield must be utilized, without exception.

When an employee leaves their work station, even for a short period of time, they must at the very least, clear the screen of any PHI. This may be accomplished by minimizing the Athena window and other programs so that only the desktop shows, or manually turning off the monitor.

It is PMA policy that anytime an employee leaves their work station for extended periods of time (i.e. to room a patient, break periods, to go to the restroom) their screen must be locked and password protected (use of control, alt, delete and “lock computer”)

Patient Exam Rooms

PMA strictly enforces signing off of athena and locking the computers in patient exam rooms before leaving the room. Under no circumstances, no matter how short the time, may an employee leave any PHI on the computer screen. If an employee needs to leave the room temporarily, it is acceptable to remain logged into athena, but the screen must be locked and password protected.

HIPAA Privacy and Procedure Policy

Password Security Policy

Implemented: March 2012

Last Updated: November 2015

Purpose: To enhance computer and user security and protection of PHI by encouraging strong and unique password creation

As a covered entity, PMA is required to have procedures in place that both prevent and authorize access to PHI on a need to know basis.

Password Best Practice Guidelines

PMA encourages employees to create unique and strong passwords both for PMA computers and third party access. The following are some guidelines to help create a secure password:

- Passwords should consist of at least 8 characters
- Passwords should incorporate all of the following: uppercase letter, lowercase letter, special symbol (like @ or $) and a number
- Passwords should not be a word that can be found in the dictionary
- Passwords should be changed at least every 60 days (if not set up automatically to do so)

Password Management

All employees are individually responsible for safeguarding their individual passwords. This means that passwords should be kept confidential and must not be accessible to anyone except the employee. This policy also applies to unique user ID login names.

- Passwords should NEVER be shared with others.
- Never use a browser's "remember password feature" for any web-based logon
- It is a violation of PMA policy to keep a copy of passwords in a place that is visible or accessible to others. (i.e. on your workstation desktop, written on sticky notes under the keyboard, on the wall)
- Passwords, if they need to be written down, must be stored in a secure place (away from your workstation desktop) and never should username and passwords be kept together on a single page. Please store usernames on one page and passwords on another and keep both pages in separate locations.
- If you choose to store your passwords electronically, they MUST be stored on your personal HIPAA compliant (H) drive and be given an obscure name (NOT passwords, logins, etc.). Additionally, this document should be password encrypted.
- Don't reuse passwords
- Don't use the same password for multiple accounts. Each account must have its own unique password
- Never email passwords or keep them stored in your email/outlook.
- If your account or password is suspected to have been compromised, notify your supervisor immediately.

It is strictly against PMA policy to store passwords on portable devices such as phone, flash drive, or laptop. It is also forbidden to take any documents containing password information outside of the office.

Employees Awaiting User Log-In Assignments

An employee, who is new to PMA or is awaiting assignment of login credentials from a third party entity, must never accept or borrow another user's ID and/or password. The following are acceptable workarounds to gain access to PHI:

- Calling the entity and properly identifying yourself, and requesting the information be faxed
- Delegating the task to another employee who can access the electronic information and manually upload to the patient's electronic chart

HIPAA Privacy and Procedure Policy

PHI Destruction Policy

Implemented: March 2012

Last Updated: November 2015

Purpose: To ensure employee understanding of proper disposal of PHI

Paper Documents

Although PMA employs the use of an electronic medical record system, it is still common to have PHI in paper form. Patient charts also fall under this policy.

It is the responsibility of each staff member to assure that all paper PHI is both secured and out of sight from other employees, patients and other individuals (i.e. pharmaceutical reps, maintenance workers).

Fax machines must be regularly checked and paper correspondence should be delivered to the addressee as soon as possible. All unclaimed faxes must be properly stored in such a way as to avoid observation by those who are not authorized.

Confidential correspondence must be placed face down or may be hidden under non-confidential papers, books, or put away in desk drawers if not in active use. Correspondence should never be left unattended in patient or other common gathering areas such as countertops and the check-out desk. Employees must also avoid leaving any PHI information in the medication storage area.

Other paper correspondence must be securely disposed of as soon as it has been uploaded into the electronic chart or when there is no more use in having it.

PMA utilizes an outside company to securely shred PHI offsite. As a business associate, they are responsible for adhering to the same privacy and security regulations as PMA. They are committed to being safe and HIPAA compliant. They provide security collection containers for convenient employee use at each office.

All paper correspondence that contains PHI MUST be disposed of in these secure containers. Correspondence with any identifiable information must never be disposed of in the trash or recycle bins.

All workstation bins used to accumulate “shredder only” documents throughout the day must be emptied into the secure shredding containers at the end of each day. Containers kept under workstations must clearly be marked as “not trash””.

Post-it notes, memo pads and personal telephone messaging notebooks may also contain PHI and must be securely disposed of in the security collection containers.

If something is accidentally disposed of in the shredder, contact your supervisor for retrieval procedure.

Electronic PHI

Scanned documents can also contain PHI. It is imperative that these documents be deleted from the scanner drive as soon as it has been uploaded to the patient's chart.

CD's containing any PHI can be put into the Pacific Records shred bin for proper disposal.

For any other devices that contain PHI, the device must be handed over to the IT manager for proper disposal. This disposal will be conducted and recorded in a HIPAA compliant manner.

It is expected that documents containing PHI will be temporarily stored on PMA computers, to complete daily tasks associated with the electronic medical record system. It is PMA policy that all documents be stored on personal (H) drives on the network rather than on the computer's desktop or documents folder. This eliminates the risk of breach in case a computer is lost or stolen. Additionally, these documents should be deleted as soon as there is no longer a business reason to keep them. Best practice is to delete the computer's recycle bin on a daily basis.

HIPAA Privacy and Procedure Policy

Fax Policy

Implemented: March 2012

Last Updated: March 2013

Purpose: To provide guidance for faxing PHI manually and electronically

Employees must take reasonable steps when faxing PHI, either manually or electronically, to ensure that it is being sent to and received by the intended recipient. From athena Clinicals, all faxes must go out through the athenaFax function so that disclosures of PHI can be properly recorded and tracked. In circumstances where transmissions through athenaFax have failed twice and the fax number is verified to be correct, manually faxing out is acceptable, only when an action note is left in the original document to note the successful manual fax transaction.

Sending Faxes by Manual Transmission

Employees must adhere to the following when sending PHI by manual fax:

- PHI is never to be disclosed on a fax cover sheet
- Use a PMA approved fax cover sheet that includes the following statement:

The PHI (Protected Health Information) contained in this FAX/Email is HIGHLY CONFIDENTIAL. It is intended for the exclusive use of the addressee. It is to be used only to aid in providing specific healthcare services to this patient. Any other use is a violation of Federal (HIPAA) and State (CMIA and IPPA) laws, and will be reported as such. If you have received this communication in error, please notify us immediately by telephone. Thank you.

- When a fax number is manually entered, the employee must double check and verify that the number entered is correct before starting transmission
- Include the name, date, telephone and fax number of the intended recipient on the fax cover sheet as well as the number of pages being sent.
- Include the sender's name and contact information on the fax cover sheet
- After transmission, verify from the fax confirmation sheet, that the transmission was successful (and note in athenaClinicals, if applicable)

Sending Faxes by Electronic Transmission

Employees must adhere to the following when sending PHI by electronic fax:

- Always double check the number in the athena global provider database. There may be multiple entries and different fax numbers may exist.
- Document in the action note area the reason for the faxed transmission
- When entering a number manually (as the recipient couldn't be found in the global data base, or the fax number is incorrect), double check the number and also indicate who the recipient is in the "to" field. Notify the Compliance Coordinator with the provider's name, address, phone and fax numbers to add to the athena database. This is critical to correctly document disclosures as required by HIPAA law.

Faxes Transmitted in Error

When an employee becomes aware that a fax was sent to the wrong number, the employee must immediately attempt to contact the recipient by fax or telephone and request that all the faxed documents be shredded, destroyed or returned.

When PMA receives notification of receipt of accidental PHI by a non PMA employee, ask the recipient to destroy all faxed documents and notify your clinic coordinator so the incident can be added to the HIPAA Breach Log. If the recipient is unable to confirm secured destruction, they may mail the records to us, C.O.D. All breaches, no matter how small, intended or not, must be communicated to the clinic coordinator as required by HIPAA law.

HIPAA Privacy and Procedure Policy

Electronic Communication Policy

Implemented: November 2015

Last Updated: November 2015

Purpose: To ensure compliance with HIPAA privacy laws regarding electronic transmission of PHI.

The following policies will be enforced for all providers and employees

Outgoing Emails

- PMA emails will not be shared with patients (exception Central Scheduling Staff limited to mailing out New Patient Paperwork)
- It is important to relay to individuals outside of PMA that our email is not secured. For all PHI correspondence, fax is the preferred method
    - Email attachments secured with passwords to open PHI sensitive documents are not considered HIPAA compliant and are not allowed to be accepted. If an email from an outside entity is received with PHI attached, please alert your supervisor so that the sender can be called to prevent further emails.
- Confidential patient records must never be attached to an outgoing email
- It is preferable to have a telephone conversation rather than e-mail any patient information
- Never include any diagnosis or other medical information or include any identifiable patient information in the subject line
    - When sending an email to another PMA employee, it is permissible to use the Patient's PMA account number in the body of the message only, and never in the subject line

Pagers

- When paging a provider for a hospital consult, through outlook, it is permissible to disclose only the patient's last name and room number.
- When paging a provider for clinic patients, only the PMA number can be disclosed. It is preferable to ask the provider to call the office if additional PHI needs to be shared. It is a violation of policy to add any other PHI (diagnosis, date of birth, etc.) to any outlook generated email.

Mobile Phones/Text Messaging

- It is strictly prohibited to store any patient information on any cellular device. Logging into athena is secure and HIPAA compliant and the preferred method of communicating patient information when a phone call is not appropriate. Athena will not store any PHI locally on any device.
- Text messaging patient information is a violation of HIPAA law unless certain safeguards are in place. At this time, PMA does not employ such safeguards. Therefore, text messaging PHI is strictly prohibited, and sanctions will be enforced for all violations.

- Employees will not use their personal cellular phones to communicate any PHI with any Provider or other employee. Communication of any patient information by text message is absolutely forbidden and sanctions will be enforced for all violations.
- In the event a PMA issued mobile phone or device is lost or stolen, IT Manger, Michael Juarez, must be notified immediately by phone so that the device can be remotely wiped to ensure there is no breach of PHI.

AthenaText Application

AthenaText is a secure and HIPAA compliant text messaging service that enables healthcare providers and authorized staff to collaborate and coordinate care via the Web in athenaClinicals and mobile phone. With AthenaText, physicians and staff members can securely communicate protected health information wherever and whenever they need to on a unified, easy-to-use platform. AthenaText is accessible after logging into Athena clinical on the web client or after entering a secure 4 digit code on the mobile app.

At this time, utilizing AthenaText to communicate PHI related messages is the approved platform that PMA employees are given permission to use. Providers are encouraged to download the AthenaText application to their phones. Staff members are permitted to use AthenaText during their normal business hours while logged into AthenaNet on their computers. Use of the AthenaText application on mobiles phones is prohibited for staff unless authorization by the Clinic Operations Manager has been given.

Laptops, tablets and other portable electronic devices

- It is strictly prohibited to store any patient information on any PMA provided portable device unless certain safeguards are employed to protect information and permission has been granted by the IT manager.
- It is a violation of PMA policy to allow anyone to store any PHI information on their own personal electronic devices.
- PMA portable devices will be reviewed and checked for PHI as determined by PMA's IT manager. Such reviews will be documented. Anyone found to have PHI stored on any device will be subject to sanctions.

CD's and Flash Drives

- CD's containing PHI, either mailed to us, brought in by a patient, or created for medical records release, will be destroyed by placing the CD's in one of the secure bins for Pacific Medical Records. These CD's will be securely destroyed.
- CD's belonging to patient may be picked up at the office, by the patient after signing a release, or they will be destroyed after 5 business days.
- CD's containing patient information should not be visible or accessible to others. They should be stored away until use and destroyed as soon as possible. CD's containing any PHI should be encrypted.
- The use of flash drives is strictly forbidden to store patient information.

HIPAA Privacy and Procedure Policy

Breach Notification Policy

Implemented: March 2013

Last Updated: November 2015

Purpose: To ensure all HIPAA breaches are reported and recorded in compliance with the requirements of the federal HITECH Act.

A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Reporting An Actual or Suspected Use or Disclosure of PHI

Any actual or suspected use or disclosure of PHI believed to be in violation of the HIPAA Privacy Rule shall be immediately reported to the clinic supervisor. The supervisors will keep a log of all events and report these to PMA's Privacy Officer on a quarterly basis for review.

In the event PMA receives notification of a suspected use or disclosure of PHI from a Business Associate, the Privacy Officer shall coordinate with the Business associate to ensure that all necessary information regarding the incident and affected patients is obtained.

Determining Whether a Breach of Unsecured PHI Occurred

Upon receiving a report of any actual or suspected unauthorized use or disclosure of PHI, the Privacy Officer shall immediately investigate the incident to determine if the incident resulted in a Breach of Unsecured PHI. The Privacy Officer shall keep the following in mind:

1. Determine whether the incident resulted in a violation of the HIPAA Privacy Rules.
2. Determine whether the incident involved "Unsecured PHI".
3. Determine whether the incident is excluded from the definition of the term "Breach"
4. Conduct a risk assessment to determine whether the incident poses a significant risk of financial, reputational or other harm to the affected patient, considering the following factors:
    a. Who impermissibly used Unsecured PHI or to whom Unsecured PHI was impermissibly disclosed;

b. Whether the immediate mitigation actions taken by PMA in response to the incident eliminated or significantly reduced the risk of harm to the affected patient;
c. Whether Unsecured PHI was returned to PMA without being accessed;
d. The nature, type and amount of Unsecured PHI that was improperly used or disclosed in connection with the incident; and
e. Any other relevant factors regarding the incident.

If, based on the risk assessment, it is determined that the incident does not pose a significant risk of financial, reputational or other harm to the affected patient, PMA, in consultation with legal counsel if appropriate, shall conclude that no Breach of Unsecured PHI has occurred and that no notification is required under this Policy.

Procedure if No Breach of Unsecured PHI Occurred

If the Privacy Officer determines that the incident did not constitute a Breach of Unsecured PHI, PMA shall document such conclusion and maintain such documentation and any supporting documents for a period of at least six (6) years from the determination.

Procedure if A Breach Of Unsecured PHI Occurred

If the privacy officer determines that a Breach of Unsecured PHI occurred, PMA shall provide notice of the Breach and maintain documentation of such notice.

Notice to Patient
Written notice of Breach shall be given to each patient whose privacy has been breached or reasonably believed to have been breached. This notice shall be provided to the patient not later than sixty (60) days after the breach is discovered. This notice shall be sent by first-class mail and addressed to the patient's last known residence or to the individual's next of kin if patient is deceased.

The notice to the patient shall contain brief details of the breach including the date of breach and the date it was discovered. It should include a description of the types of PHI that were disclosed, how the patient can protect themselves, update as to what PMA is doing to investigate and mitigate harm to the patient and contact information for the patient to ask questions.

This notice should also be posted on the PMA website in the event that 10 or more patients could not be notified by mail or by phone.

Notice to HHS

In addition to notifying the patient, PMA shall notify HHS of the Breach if it involves 500 or more patients without unreasonable delay and no later than 60 days of the discovery.

If the breach involves less than 500 patients, PMA will submit the maintained log of breaches to HHS no later than 60 days after the end of each calendar year.

Notice to Media

If a Breach involves 500 or more patients of a certain state or city, PMA must also notify prominent media outlets serving that state or city. This notice must be provided no later than 60 days from discovery and include the same information included in the notice to the patient.

Documentation of Breach Notice

PMA shall maintain the documentation of all suspected and reported breaches. Each clinic supervisor is responsible for maintaining the log. All breaches should be reported to PMA's Privacy Officer for further investigation to determine if a breach of Unsecured PHI has occurred. A log of all PHI breaches must be submitted to DHHS within 60 days of the end of the calendar year.

pma

HIPAA Privacy and Procedure Policy

Contingency Plan for EHR Downtime

Implemented: March 2013

Last Updated: November 2015

Purpose: To prepare staff to continue with a patient visit, in the event our EMR system (athenaNet) is not available

It is the policy of Pulmonary Medicine Associates (PMA) to have procedures in place to support the continuation of safe patient care during downtime of clinical systems. PMA managers will prepare and maintain supplies needed to maintain clinic operation in the event of Electronic Medical Record downtime.

There may be situations in which our EMR system may be down during office hours (due to vendor downtime, loss of internet use, power outages, etc.) and we are unable to access medical records when patients are in the office. The following is a contingency plan that will assist staff and Providers with uninterrupted patient care, and to preserve the integrity of PHI. This plan will be in effect until connection with athenaNet is restored.

1. Confirm the system is down and connection is lost (i.e. cannot log into athenaNet, or system is unavailable)

2. Verify the internet is functional by attempting to access www.pmamed.net.
    a. If the internet is unavailable, immediately notify the I.T manager or designee
    b. If the internet is available, but the EMR system is not responding, notify the Clinic Operations Manager, Compliance Coordinator or designee.

3. The Office Coordinator or designee will make direct contact with each provider and staff member to inform them the office is instituting downtime procedure for the Electronic Medical Record.

4. Patients will need to be alerted that our EMR system is down and that access to their charts is temporarily not available, in which case they may be asked about their history or other information that is not readily accessible.

5. In case of a power outage, if no power has returned within 30 minutes, those patients who are waiting to see their provider, will need to have their appointment rescheduled. Staff will recall all patients who were sent home with a new appointment date/time.

6. Distribute downtime backup encounter forms. This form can be found in the “Compliance” (I) drive, specifically in the “athena” folder under “blank paper encounter (EHR downtime)”. All staff handling patient related information must document on downtime forms.

7. Instruct Providers and staff to use the following methods for orders that must be carried out immediately:
    a. Visit notes must be hand written
    b. Providers will need to use paper RX pads to create orders/write drug prescriptions. Orders can be transmitted by telephone or fax if service is

available. Medical assistants may not telephone in new prescriptions or prescriptions refills that include any changes from the previous order.

c. Lab and Radiology requisitions may be completed on paper referrals, and given directly to the patient or transmitted by fax if available.
d. Copies of anything given to the patient will need to be attached to the paper encounter and scanned into the patient chart when the system is restored.

8. There is a section on the paper encounter that allows the provider to note the return date for the patient's follow up. Check out staff will inform patients they will call them back with any status to their tests, authorizations, and to schedule their next appointment.

9. When the system is restored, resume normal documentation.

10. When access to athena is restored, all paper encounter forms will need to be transferred to the encounter for the date of service. The staff will be responsible for inputting their information (Intake) taken on the paper form into athena. The paper form has a check mark box available to mark when sections are successfully added to the electronic chart. Providers will also need to finish their documentation and orders and enter any CPT and ICD-10 codes.

11. Provide all downtime forms to medical records for scanning into the patient charts. It will be added as "Encounter Document – Progress Note. Note: This can only be attached after the encounter is in **CLOSED** status.

HIPAA Privacy and Procedure Policy

PHI Access Termination Policy

Implemented: March 2013

Last Updated: November 2015

Purpose: To terminate an employee's access to PMA's information assets and to any third party program where PHI is accessible to prevent HIPAA breaches

A termination checklist for each employee must be completed to ensure all termination procedures are completed. This form is accessible electronically to those responsible for assigning and revoking accesses. This checklist will remain in the employee's file after termination.

1. Human Resources will need to alert the following people of the termination of any PMA employee so that termination procedures may be carried out. Each of the individuals stated below has certain steps to take to ensure all access is revoked immediately:
    a. IT Officer
    b. Billing Manager
    c. Supervisors

2. The IT Manager will ensure that ALL user access has been disabled from the PMA network including access to outlook and will provide an anticipated file destruction date. Any portable equipment loaned to the employee (i.e. Pagers, Laptops, Cell Phones) will be collected.

3. The Billing Manager will ensure that access to athena, MedAptus and all insurance sites that the employee used as part of their duties will be disabled.

4. Supervisors will ensure that ALL user access has been disabled for all 3rd Party clinical PHI sites, as well as collect ID badges, tokens, keys, etc. The supervisor will also ensure that all user access has been disabled for alarm codes, staples/office max and pacific records. Additionally, if the employee had passwords written on paper, those must be collected and properly shred.

5. When the terminated individual was responsible for the creation, removal or maintenance of User IDs from any system, Management should immediately remove their access and assign a new or temporary employee for those duties.

6. A terminated employee's computer files will be retained for (4) weeks after the user has permanently left PMA. Access to those files for any reason may only be granted with the permission of the Chief Privacy Officer.

HIPAA Privacy and Procedure Policy

Medical Records Retention Policy (NEW)

Implemented: November 1, 2018

Last Updated: November 1, 2018

Purpose: To outline the retention period for medical records and to establish conditions and time periods for which medical records will be stored, retained, and/or destroyed after they are no longer active for patient care or business purposes and to ensure appropriate availability of medical records.

Medical Records shall be maintained and retained on an ongoing basis to ensure they are current, detailed and organized. PMA will adhere to retention schedules and destruction procedures in compliance with regulatory, business and legal requirements.

As of 04/01/2011, PMA creates and maintains all medical records in an electronic format, stored with our current EMR vendor, Athenahealth. Any record created, received or maintained before 04/01/2011 has been stored in a paper chart.

Retention of Paper Records (Charts):

1. Charts shall be retained for seven (7) years after the last ambulatory encounter.
2. Under no circumstances shall any paper record be destroyed before seven (7) years after the last ambulatory encounter.

Storage of Paper Records (Charts):

1. Charts will be stored at an off-site facility that has been approved for record storage according to HIPAA laws. PMA will keep a current BAA (Business Associate Agreement) on file with the approved facility, currently Pacific Records Management.
2. Charts will be kept in numbered boxes that will be picked up and stored off-site by the approved facility mentioned above. The box number where the chart is filed will be noted in the patient's electronic chart for reference.

Destruction of Paper Records (Charts):

1. Charts will be individually reviewed before destruction to ensure it will not be prematurely destroyed.
2. Charts approved for destruction will be destroyed by the off- site facility. A receipt will be given to confirm the secure destruction of those charts.
3. The following will be noted in the electronic chart "Paper Chart Destroyed on XX/XX/XXX" for compliance purposes.
4. The Paper Chart destruction date will be provided when an authorized request for medical records in received.

PMA currently plans to retain all information created and maintained in the electronic chart after 04/01/2011 indefinitely.

Other Records in electronic format, created by PMA and stored on PMA servers, shall be destroyed at company discretion but no sooner than seven (7) years after creation date.

Other records on electronic media (CDs) will be returned to patient and/or destroyed after 30 days. PMA does not store or maintain films or CDs with PHI.

HIPAA Privacy and Procedure Policy

Title: Confirmation of Receipt

I understand that protecting the privacy of patients' protected health information is of the upmost importance to Pulmonary Medicine, Infectious Disease, and Critical Care Consultants Medical Group, Inc.

I have received a copy of Pulmonary Medicine's HIPAA Privacy and Security Policy and Procedure, as well as training related to my responsibilities for keeping patient information private. I acknowledge that it is my responsibility to read and understand the policies and procedures contained in the Policy.

I acknowledge that I have been informed that I can be subject to disciplinary action if I fail to comply with the Privacy and Procedure Policy.

I have had an opportunity to ask any questions regarding PMA's HIPAA Privacy and Security Policy and Procedure, and I commit to asking my supervisor or PMA's Privacy Officer any related questions that may come up in the future, or if I am unsure how to proceed with my work related to this topic. I have been informed who PMA's Privacy officer is.

Employee's Name (print): _____

Employee's Signature: _____

Date: _____

Review Documentation

Review Date	Reviewed By	Approved by		Review Date	Reviewed By	Approved By
03/2012	Compliance Coordinator	Chief Privacy Officer				
03/2013	Compliance Coordinator	Chief Privacy Officer				
03/2014	Compliance Coordinator	Chief Privacy Officer				
10/2015	Compliance Coordinator	Chief Privacy Officer				
12/2016	Compliance Coordinator	Chief Privacy Officer				
08/2017	Compliance Coordinator	Chief Privacy Officer				
11/2018	Compliance Coordinator	Chief Privacy Officer				
10/30/2019	Compliance Coordinator	Chief Privacy Officer				