HIPAA Privacy and Procedure Policy
Pulmonary Medicine Associates

Effective 01/01/2012
Revised 11/25/2022
Version# 22.1

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 the electronic exchange of health information nationally 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.

To strengthen the privacy and security protections for health information established under HIPAA, the Final Omnibus Rule dramatically 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 guide 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 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. The protection of patient privacy is of supreme importance to this organization. Violations of these procedures and policies may result in disciplinary action, 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 the PMA employee handbook.

Contact

Chief Privacy Officer: **Tim Short, Chief Operations Officer**
1300 Ethan Way, STE 600
Sacramento, CA 95825
Phone (916) 679-3540 | fax (916) 483-0814
tshort@pmamed.com

Compliance Supervisor: **Christina Torres**
1300 Ethan Way, Suite 600
Sacramento, CA 95825
Phone (916) 679-3546 | fax: (916) 483-0814
ctorres@pmamed.com

Definitions

1. "**Patient**" means any person who has registered and has received services at PMA without regard to the 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. "**Covered Entities**" are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) medical care providers who electronically transmit any health information. Covered entities can be institutions, organizations, or persons.

4. "**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.

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

6. "**Workstation**" means the principal 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, tablets, and smartphones.

Please get in touch with the Compliance Supervisor listed above if you have any questions about the information in this policy or any HIPAA regulation.

Policy Section

HIPAA Privacy and Procedure Policy

Notice of Privacy Practices (NOPP)

Implemented: March 2012

Last Updated: October 2021

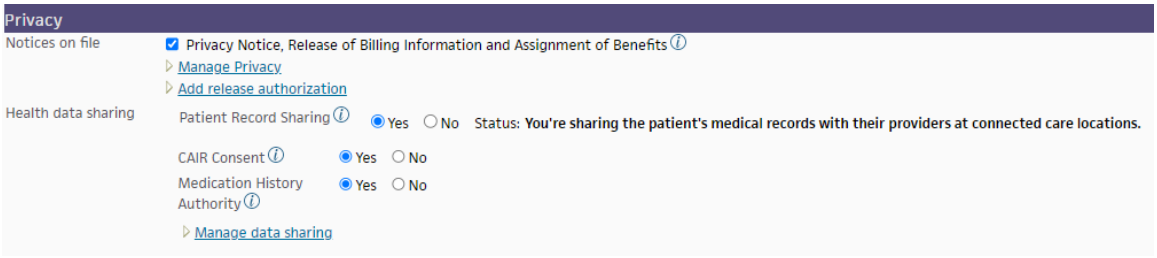
Purpose: To provide guidance in understanding PMA's Notice of Privacy Practices (NOPP)

The *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 in which patients request that their health benefit payments be made directly to PMA. Downloading a patient's medical record, including medication and vaccine histories, via an interface is also covered under this notice. PMA's policy is to offer patients a copy of the NOPP at each visit at check-in.

This notice is initially provided to the patient with their New Patient Welcome Packet or no later than the date of their first visit. It is also available to patients on their patient portal and the company website (www.pmamed.com). A copy of the NOPP will also be posted in the office or clinic lobby.

The law requires us to ask patients to state that they received this notice in writing. However, patients are not required to sign this acknowledgment, and we must record any refusal in the chart. Check-in staff is expected to review the registration form for appropriate authorization. Refusing to sign will not prevent a patient from being seen or prevent us from using or disclosing health information where HIPAA permits. When the NOPP is given to the patient, and the patient refuses to sign, staff should make a notation on the patient's registration form and upload it to the patient's chart.

Privacy Notice, Release of Billing Information and Assignment of Benefits, Patient Record Sharing, CAIR Consent, Medication History Authority, and Consent to Call in Athena



It is permissible for staff to check the appropriate boxes within the Quickview screen at check-in after the patient has acknowledged receipt for or has been provided the NOPP. These boxes should also be checked after a patient's refusal has been documented.

We must get the patient's verbal consent to receive automated calls (Athena Communicator) to their mobile phone, as HIPAA law does not cover this. A yes answer for the "consent to call" box should only be chosen if the patient consents to receive automated calls directly to their mobile phone. This consent may be verbal.

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 provide individuals with certain rights to their health information. Examples of entities include healthcare providers, health plans, and healthcare clearinghouses.

The following is a sample list of entities for which additional consent from patients is not necessary before 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 can add an Emergency Contact to their new patient registration sheet. It is important that only the person listed by the patient in writing be added to the Emergency Contact fields in the EHR. This information needs to be verified at the time of check-in. The patient must consent to the following clause that relates only 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. Patients may restrict disclosures to their health plans if they pay 100% of their services out of pocket. The patient must provide this restriction in writing and make arrangements with the Billing Services Manager.
See Policy for Release of Medical Records for more information.

Patient Portal

A Web-based Patient Portal gives patients secure and convenient access to their health information. Patients can use the Patient Portal to view, download, transmit their health information, and send secure messages to their providers.

We invite patients to register for an account using their own e-mail addresses. Patients are welcome to register family members as long as we have that authorization in writing. Because HIPAA law requires us to differentiate who is accessing patient information, staff should ensure they correctly indicate whether the patient portal account belongs to the patient or another person.

Granting Patient Portal Access:

- Once a patient's identity has been verified, only the patient can verbally offer their e-mail address over the phone to be set up to access their portal.
- We cannot collect e-mail addresses from anyone other than the patient (or legal representative) to add as a chart contact.

- A patient may verbally authorize another individual to access their portal on their behalf. In this situation, the patient must know and provide that individual's name, phone, and e-mail. Staff must explain to the patient that granting portal access to others will allow them to see their personal medical information online. Only with the patient's understanding and verbal agreement should we continue with adding that individual as a patient contact.
- If a patient cannot give verbal authorization (e.g., language barrier, non-verbal, etc.), we cannot grant anyone access to the portal, even if the caller says the e-mail belongs to the patient.
- When the patient presents for their visit, check-in staff should verify that all individuals granted portal access are listed on the registration form. If this information is not provided or collected, those individuals should have portal access revoked immediately.

HIPAA Privacy and Procedure Policy

Release of Medical Records Policy

Implemented: March 2012

Last Updated: November 2020

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 Compliance Supervisor.

Please have patients fill out the PMA Authorization to Release Medical Records Form for all consented disclosures.

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

- The purpose for release;
- Specific information being requested;
- Dates of records requested; and
- Explicit permission for special consents (if applicable)
- Signature and date

HIPAA outlines that the authorization is invalid if it is not filled out completely. Furthermore, we cannot honor "blank" releases as HIPAA does not permit modification of the release by anyone other than the patient or authorized individual after the form has been signed.

We can only accept authorizations signed by the patient or their guardian. If an individual has the legal authority to sign on behalf of the patient, documented proof must accompany the signed release form.

Release of Electronic or Paper Requests for Copies of Medical Records of PMA Clinic Patients

Identity Verification

The HIPAA privacy rule requires documented verification of the identity and authority of a person requesting protected health information. All persons authorized to pick up records must also provide proof of identity. The following is a list of guidelines for identity verification:

- Patients: Patients should provide a photo ID when signing a release or picking up a copy of their records. For signed releases received by mail or fax, the patient's signature on the form should match the signature recorded in the patient's medical record. There should be no question that the patient is the individual who has signed the release.
- Legally Authorized Representative: If a legally authorized representative of a patient makes a request, confirm that they are the patient's legal representative in the medical record (we should have a copy of legal documents). They must present a photo ID, a valid power of attorney for health care, a court order, or other verification of their identity and authority as a representative.
- Subpoenas or Legal Requests: These must always be served in person and be accompanied by court orders, and medical record staff will verify the validity of the request. Courier companies who pick up completed requests should present a photo ID, company badge, and correspondence containing patient information.

- Minor: A person requesting on behalf of a minor should present a photo ID and a birth certificate, power of attorney, letter of guardianship, court order, or other evidence of their relationship to the minor and/or their authority to act on the minor's behalf.
- Patient Portal: Staff is to ensure that requests from the patient portal are indeed being initiated by the patient (and not coming from a family member's portal account unless we have documentation of their legal authority to do so).

We are required to honor a patient's request for an electronic copy of their 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 three days of the request for electronic records and 15 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 responsible for protecting patient privacy as HIPAA law documents. With written authorization from the patient, paper records containing less than 25 pages may be mailed. Additional delivery arrangements can be made with approval from the Medical Records Supervisor.

Due to the time-sensitive nature 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 can also collect any fees associated with the release for a quicker turnaround.

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

It is permissible to publish medical records 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. Although publishing these to the Patient's Portal is preferable, we can provide a paper copy if the patient requests. This disclosure must be done through chart export to document it in athena correctly. Any time a patient requests more information than can be published to the portal or any more than two items, the patient must sign a release of records, and the medical records staff will process their record request.

Before releasing paper copies of medical records to the patient or other authorized person, PMA's policy is to have at least one of the following:

- Release of Medical Records Request form completed and signed by the patient (or patient's legal representative) 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 "Admin-Medical Records Request" classification. 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 has been disclosed is recorded in the medical record. This is necessary to maintain a precise Accounting of Disclosures.

Paper Record Transfers To Clinics

For inter-office transfers within PMA, any printed or unencrypted electronic 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 any PMA office, hospital, or facility.

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 written authorization to release information, we must fulfill that request if we have such records on file. However, PMA's policy is to assist and encourage the patient to request records through the rendering facility, as our records may be incomplete.

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 medical information to any other entity or person without a signed subpoena, court order, or other official document permitting such release.

New HIPAA regulations permit PHI to be verbally communicated to persons or entities that would have been covered if the patient were living. Communication related to treatment, payment, or healthcare operations is permitted if the patient did not make such restrictions before death. However, this does not apply to releasing physical paper or electronic records.

All HIPAA release forms and the powers they grant expire upon a patient's death, as do the rights conveyed by a Medical Power of Attorney. Only the patient's designated "personal representative" can access the deceased person's medical record under the law. The law does not give any other person the right to access 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 they 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 are sufficient to establish one's right. In most cases, the next of kin or surviving spouse is acceptable.

Disclosures Requiring Special Consent

For PMA to disclose Highly Confidential Information for purposes unrelated to treatment, payment, or healthcare operations, we must obtain a patient's separate and specific written consent. Highly confidential information includes Drug and 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 disclosures. Patients must initial those sections on the form for the release to be valid.

Documenting Authorizations to Obtain and Disclose Health Information in Athena

The individual listed by the patient on their registration form as their emergency contact will be recorded on the full registration page in Athena. This form will be uploaded into the patient chart and adequately 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 shall also be added to the "Patient Care Team" section within the athena chart.

Patient Right to Inspect and Copy

Patients have the right to inspect and copy their medical record information, including medical and billing records. Patients must submit their request in writing to the PMA Medical Records Department.

This request may be denied if the patient requests 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 will be forwarded to the usual provider for approval or the Compliance Supervisor if the usual provider is no longer with PMA.

If denied, the patient may request the denial be reviewed, and PMA will choose another licensed healthcare professional to proceed with the review. All patient requests for their denial to be reviewed will be forwarded to the Compliance Supervisor.

Patient's Right to Amend

If a patient believes the information included in their medical record is incorrect or incomplete, they may ask us to amend it. This request must be made in writing and 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;
- PMA did not create the information 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 they were permitted to inspect and copy; or
- The information is found to be accurate and complete

These requests are to be forwarded to the usual provider for review or to the Compliance Supervisor if the usual provider is no longer with PMA.

If the request is denied, a patient may still submit a written addendum that does not exceed 250 words for 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 included whenever PMA discloses 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 disclosure in writing to the PMA Medical Records Department. The request must provide a date range and preferred method of disclosure (paper or electronic) and 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 person 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 entire care out-of-pocket and have 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 restrict
- Whether this is to limit the use 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 Compliance Supervisor.

Patient Rights to Confidential Communications

Patients have the right to request that we communicate with them about medical matters in a certain way or at a specific location. For example, patients can ask that we only contact them at home 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 electronic chart.

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

PMA's policy is 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 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 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 Compliance Supervisor.

Fees

The medical records supervisor creates and maintains a fee schedule for disclosing medical records as allowed per applicable state and federal laws and regulations.

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 medical records or records they don't have a business reason to access

All covered entities, including Sutter, Mercy, and PMA, must have procedures that prevent unauthorized access to medical records and prevent employee access to their personal medical records using company-provided access. 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, Dignity, imaging, and lab vendors.

- PMA workforce members may only access files or programs, whether computerized or otherwise, that are necessary to perform their immediate job functions. Unauthorized review, duplication, dissemination, removal, damage, or alteration of files, passwords, computer systems, 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 circumstance, use PMA equipment or assigned credential to access any medical record, including personal records, 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 online portals of other medical entities using their own credentials for personal reasons.

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 requesting PHI, the 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 a medical record. PHI also includes financial, demographic, and lifestyle information. This includes paper, electronic, and spoken communication.

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 required to satisfy a particular purpose or carry out a specific function.

This policy does not impede access to patient information necessary for healthcare providers to make medical decisions and provide treatment to patients 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 under 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 responsibilities.

Need to Know Principle

PMA workforce members are not permitted to access the PHI of a patient unless there is a 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 discuss patient information with other PMA staff who do not need to know.

HIPAA Privacy and Procedure Policy

Telephone and Office Privacy Policy

Implemented: March 2012

Last Updated: December 2020

Purpose: To provide the PMA workforce with general guidelines for PHI communication by telephone and in the office environment

Telephone Privacy Procedures:

PMA requires its employees to always verify a patient's or caller's identity whenever PHI is discussed. Name, date of birth, and another demographic would suffice requirements (e.g., telephone number, address). Never provide PHI for the patient to verify; instead, ask them to give the information to you.

PMA employees can communicate the following information to any individual who answers a call to a patient's phone number on file. Messages may be left on a voice answering device or with a physical person, authorized or not, indicating the following:

- Employee's first name, title, and company or provider name
- Appointment confirmation/reminder
- A message to have the patient call the office
- Clinic phone number and address

Front Office / Central Scheduling staff may only discuss with the patient OR their emergency contact OR other individuals that the patient has given verbal or written consent to disclose medical/financial information:

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

Appointments can be scheduled by individuals other than the patients; however, diagnosis or specific appointment reasons should not be disclosed unless the patient has authorized the individual to receive such information.

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

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

Medical Records Staff may only discuss with the patient OR their emergency contact OR other individuals that the patient has given verbal or written consent to disclose medical/financial information:

- Dates of office visits or other in-house procedures
- Availability of Records

Billing Staff may only discuss with the patient OR their emergency contact OR other individuals that the patient has given verbal or 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 information required to complete proper billing procedures
- Balance due and current status of the account

After identity verification, the billing staff should not discuss any medical diagnosis or information with anyone other than the patient or a legally authorized representative.

If the nature of the call concerns 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. After conducting an identity verification, it is best to discuss billing-related concerns with the patient whenever possible.

Medical Assistants may only discuss with the patient OR their emergency contact OR other individuals that the patient has given verbal or 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 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 leave a message that recent tests were normal but not say what testing was done on a voicemail. 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. In addition, this must fully be documented in the document action notes or other acceptable fields in athena, including the patient's verbal consent details.

Office Privacy Procedures:

Discussion of PHI between patients, 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 walk to the person so the discussion can be private, or the phone should be utilized.

Voice should be kept at the lowest level possible when on the phone. If a patient or other parties may be hard of hearing, it is advisable to ask if they may be placed on hold while the staff changes phones to 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. When two or more people are checked in with the same last name, it is permissible to include the first name. 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 the PMA workforce with proper safeguarding of workstations to prevent unauthorized use and to protect PHI

Desks

The IT Department Manager shall assign all employees log-on credentials to use their workstation computers, access e-mail and secure network drives.

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, they must, at the very least, clear the screen of any PHI. This may be accomplished by minimizing the EMR window and other programs so that only the desktop shows. Manually turning off the monitor would suffice as well.

It is PMA policy that anytime an employee leaves their work station for extended periods (e.g., to room a patient, take breaks), their PC 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 unlocked computer with a patient unattended.

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 for PMA computers and third-party access. The following are some guidelines to help create a secure password:

- Passwords should consist of at least eight characters
- Passwords should incorporate all of the following: an uppercase letter, a lowercase letter, a 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 passwords. This means that passwords should be kept confidential and must not be accessible to anyone else. This policy also applies to unique user ID log-in names.

- Passwords should NEVER be shared with others
- Never use a browser's "remember password feature" for any web-based log-on
- It is a violation of PMA policy to keep a copy of passwords in a place that is visible or accessible to others. (e.g., on your workstation desktop, written on sticky notes under the keyboard, on the wall)
- If they need to be written down, passwords must be stored in a secure place (away from your workstation desktop), and never should usernames 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, log-ins, 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 a unique password
- Never e-mail passwords or keep them stored in your e-mail/outlook
- If your account or password is suspected of being compromised, notify your supervisor immediately

It is strictly against PMA policy to store passwords on portable devices such as phones, flash drives, or laptops. It is also forbidden to take any paper documents containing password information outside the office.

Employees Awaiting User Log-In Assignments

An employee, who is new to PMA or is awaiting the assignment of log-in credentials from a third-party entity, must never accept or borrow another user's ID 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 it 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 an electronic medical record system, having PHI on paper is expected. Patient charts also fall under this policy.

PMA employees must adhere to a "clean desk" policy. A clean desk means that employees must clear their desks of any PHI and sensitive paper documents at the end of their workday. Each staff member's responsibility is to ensure that all paper PHI is secured and out of sight from other employees, patients, and other individuals (e.g., pharmaceutical reps and 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 appropriately stored in such a way as to avoid observation by those who are not authorized.

Confidential correspondence must be placed face down or under non-confidential papers or books or put away in desk drawers if not in active use. Correspondence should never be left unattended in 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 business use for having it.

PMA utilizes an outside company to shred PHI off-site securely. As Business Associates, they adhere 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 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 a retrieval procedure.

Electronic PHI

Scanned documents can also contain PHI. These documents must be deleted from the scanner drive as soon as it has been uploaded to the patient's chart.

CDs containing any PHI can be put into the secure 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. PMA policy requires that all documents be stored on personal (H:) drives on the network rather than on the computer's desktop or documents folder. This helps mitigate the risk of a breach if 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. The best practice is to delete the computer's recycle bin daily.

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/E-mail is HIGHLY CONFIDENTIAL. It is intended for the exclusive use of the addressee. It is to be used only to provide specific healthcare services to this patient. Any other use violates Federal (HIPAA) and State (CMIA and IIPPA) laws and will be reported as such. Please notify us by telephone if you have received this communication in error. Thank you.

- When a fax number is manually entered, the employee must double-check and verify that the number entered is correct before starting the transmission
- Include the name, date, telephone, and fax number of the intended recipient on the fax cover sheet and 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 the EMR, 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 EMR global provider database. There may be multiple entries, and different fax numbers may exist
- Document the reason for the faxed transmission in the action note area of the document in athena.
- When entering a number manually (as the recipient couldn't be found in the global database or the fax number is incorrect), double-check the number and indicate who the recipient is in the "to" field. Notify the Compliance Supervisor of the provider's name, address, phone, and fax numbers to add to the athena database. This is critical to document disclosures as required by HIPAA law
- All updates to entity contact information should be directed to the Compliance Supervisor

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 the notification of the receipt of accidental PHI by a non-PMA employee, ask the recipient to destroy all faxed documents and notify your clinic supervisor so the incident can be added to the HIPAA Breach Log. If the recipient cannot confirm secure destruction, they may mail the records by C.O.D. No matter how small, intended, or not, all breaches must be communicated to the clinic supervisor as required by HIPAA law.

HIPAA Privacy and Procedure Policy

Electronic Communication Policy

Implemented: November 2015

Last Updated: October 2021

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

PMA has adopted policies to comply with federal and state privacy laws and regulations. As a healthcare organization, it is critical that we ensure the integrity and confidentiality of patient information, protected health information (PHI), and data/information related to Pulmonary Medicine Associates (PMA), whether in oral, written, electronic, or any other form. It is also important to understand that a privacy violation can result in civil and criminal penalties; employees can be held personally liable for their actions and face fines and prison time. The following policies will be enforced for all providers and employees

Outgoing E-mails

- Sending any PHI or confidential data outside of the PMA network without encryption is prohibited
- It is a violation of PMA policy to e-mail any patient information outside of the PMA network (unless noted by exception)
- PMA e-mails will not be shared with patients (unless noted by exception or written policy)
- It is important to relay to individuals outside of PMA that our e-mail is not secure. For all PHI correspondence, fax is the preferred method
- Confidential patient records must never be added or attached to an outgoing e-mail
- It is preferable to have a telephone conversation rather than e-mail any patient information
- Never include any diagnosis or other medical information or have any identifiable patient information in the subject line
    - When sending an e-mail 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
- Transmission of PHI using personal e-mails is prohibited
- Transmitting or forwarding confidential information to outside individuals not authorized to receive such information or to other PMA employees who have no business or clinical reason for such information is also prohibited

Storage of e-PHI

- All data created by employees of PMA is the property of PMA
- All PHI must remain stored on PMA's secured network
- Storage of PHI or other confidential data on an external site (e.g., google drive, dropbox) is not approved for PMA employee use
- Employees who work from home may not download or save any confidential information to their local computer or cloud-based storage

Pagers

- When paging a provider for a hospital consult, it is permissible to disclose only the patient's last name and room number through outlook
- 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 violates policy to add any other PHI (diagnosis, date of birth, etc.) to any outlook generated e-mail

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 inappropriate. Athena will not store any PHI locally on any device.
- Text messaging patient information violates 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.
- If a PMA-issued mobile phone or device is lost or stolen, the IT Manager 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 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 on the web client or after entering a secure four-digit code on the mobile app.

At this time, utilizing AthenaText to communicate PHI-related messages is the approved platform that PMA employees can use. Providers are encouraged to download the AthenaText application to their phones. Staff members can use AthenaText during regular business hours while logged into AthenaNet on their computers. Use of the AthenaText application on personal mobile phones is prohibited for staff unless authorized by the Clinic Operations Manager.

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 data and permission has been granted by the IT manager.
- It violates PMA policy to allow anyone to store PHI information on their 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.

CDs and Flash Drives

- CDs containing PHI, either mailed to us, brought in by a patient, or created for a medical records release, will be destroyed by placing the CDs in one of the secure bins for Pacific Medical Records.
- After signing a release, the patient may pick up their CDs, or they will be destroyed after five business days.
- CDs containing patient information should not be visible or accessible to others. They should be stored away until used and destroyed as soon as possible. CDs containing any PHI must be encrypted.
- The use of flash drives is strictly forbidden to store patient information.

Monitoring, Enforcement, and Sanctions

- PMA actively monitors activity and data stored on its network and devices.
- There should be no expectation of privacy on PMA equipment; all data stored on PMAs network, applications, devices, etc., are discoverable.
- Employees should understand that computer activities create audit trails and that deleted, edited, and overwritten computer files often cannot be erased or may be recovered using cyber forensic techniques.
- Employees must immediately report any suspected or known violations of any PMA policy or breach of patient information.
- PMA reserves the right to revoke any user's access to the network at any time.
- Failure to follow any policy and procedure will result in disciplinary action, up to and including **immediate termination and legal action**

pma

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

Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information. 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 violate 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 the Compliance Supervisor immediately for review.

If PMA receives the 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 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 the individual's next of kin if the patient is deceased.

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

This notice should also be posted on the PMA website if ten or more patients cannot be notified by mail or 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 contained 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.

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

PMA's policy is to have procedures to support the continuation of safe patient care during the downtime of clinical systems. PMA managers will prepare and maintain supplies needed to maintain clinic operation during 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 cannot 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 preserve the integrity of PHI. This plan will be in effect until the connection with the EHR is restored.

1. Confirm the system is down and the connection is lost (e.g., cannot log into EMR, or the 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 IT manager or designee
    b. If the internet is available, but the EMR system is not responding, notify the Clinic Operations Manager, Compliance Supervisor, or another designee.

3. The Office Supervisor will inform each provider and staff member that the office is instituting a 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 unavailable, 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, patients waiting to see their provider will need to reschedule their appointment. 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 the 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 handwritten
    b. Providers must 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 prescription refills that include 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 must be attached to the paper encounter and scanned into the patient chart when the system is restored.

8. A section on the paper encounter 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 of their tests and authorizations and to schedule their next appointment.

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

10. When access to the EMR 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 checkmark box to mark when sections are successfully added to the electronic chart. Providers must also finish 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 a **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 specific 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 outlook access, and provide an anticipated file destruction date. Any portable equipment loaned to the employee (e.g., 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 and collect ID badges, tokens, keys, etc. The supervisor will also ensure that all user access has been disabled for alarm codes, supply websites, and pacific records. Additionally, if the employee had passwords written on paper, those must be collected and securely shredded.

5. When the terminated individual was responsible for creating, removing, or maintaining 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

Implemented: November 1, 2018

Last Updated: November 1, 2018

Purpose: To outline the retention period for medical records, establish conditions and time periods for which medical records will be stored, retained, and destroyed after they are no longer active for patient care or business purposes, and 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. After the last ambulatory encounter, charts shall be retained for seven (7) years.
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 they 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 is received.

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

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

Other records on electronic media (CDs) will be returned to the patient 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 utmost 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 and 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. I also commit to asking my supervisor or PMA's Compliance Supervisor any related questions that may come up in the future or if 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: _____

pma

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				
10/30/2020	Compliance Supervisor	Chief Privacy Officer				
10/29/2021	Compliance Supervisor	Chief Privacy Officer				
11/25/2022	Compliance Supervisor	Chief Privacy Officer				