



Pacific Medical Centers HIPAA Training for Residents, Fellows and Others

Summary of Critical Pacific Medical Centers (PMC) HIPAA Policies and Procedures

For additional information or questions, please contact the clinic director or the PMC Privacy Office at (206) 621-4678. Complete policies and procedures can be viewed on The Pac, PMC's intranet site or obtained from the clinic director.

Uses and Disclosures of Protected Health Information (PHI) Requiring Authorization

Uses and Disclosures of PHI without Authorization to External Parties

Use and Disclosure of PHI without Authorization for Legal Purposes

Policy:

PMC needs an individual's valid authorization for use and disclosure of PHI. There are circumstances when an individual's authorization is not necessary for use and disclosure of PHI.

Overview:

Best to involve the clinic's Health Data Services Department or clinic director when dealing with authorizations.

PMC must report:

1. Cases of abuse or neglect of any child under the age of eighteen to the appropriate authorities at the first opportunity (but within 48 hours).
2. Disease, injury, disability to public health authorities to protect the public health or if authorized by law.

Complaints Related to Pacific Medical Centers' Privacy Practices

Policy:

Patients, their families or PMC workforce members have the right to make a complaint related to PMC privacy practices in writing, by phone or in person.

Overview:

To file a complaint or comment, individuals can contact:

1. Any clinic employee
2. The PMC Privacy Officer at (206) 621-4678
3. Washington State Department of Health

Consent for Treatment, Payment and Healthcare Operations (TPO)

Policy:

1. PMC will obtain an individual patient's consent prior to using or disclosing his/her PHI for treatment, payment or healthcare operations for its own use except when
 - The provider has a direct or indirect treatment relationship with the individual patient
 - Another health care staff member is assisting the provider in the delivery of health and the provider reasonably believes that the staff member will not use or disclose the PHI and will protect that information
 - A consent for TPO will not be in effect if an authorization is required or when another condition must be met to permit use or disclosure of PHI
 - PMC may disclose PHI for treatment or payment activities to another covered entity or health care provider of the covered entity
2. PMC may disclose PHI to another covered entity for health care operations activities if:
 - They have a relationship with the individual patient
 - The PHI pertains to the relationship
 - The disclosure is for the purpose of
 - a. QA and improvement activities
 - b. Population-based activities for improving health or reducing costs
 - c. Case management or care coordination
 - d. Training programs
 - e. Accreditation, licensing or credentialing activities OR
For fraud and abuse detection or compliance activities

Copying and Printing PHI

Policy:

Guidelines pertaining to copying or printing original or duplicate copies of PHI.

Overview:

1. There should be a legitimate business or patient care purpose for reproducing PHI.
2. Reproduced copies of PHI should be stored in a secure location.
3. Printing and copying should occur in private areas not accessible to the public.
4. Reproduced copies should be promptly removed from copiers and printers.
5. Disposal of reproduced copies should follow the Disposal of PHI policy.

Disposal of Protected Health Information (PHI)

Policy:

PMC is obligated to protect the confidentiality of PHI

Overview:

1. Workforce members must dispose of PHI in the appropriate containers at each clinic. Clinic employees can assist in determining how to dispose of any PHI.
2. Electronic media that contains PHI must be sent to Information Services for proper disposal.

Use of Email for Business Purposes

Policy:

1. For new patients registered after April 14, 2003, do not send confidential or patient identifiable information by email across external or public networks (e.g. Internet).
2. For existing PMC patients where email communications are currently occurring such communications can continue to occur as long as the following disclaimer statement is included for all external emails sent:
CONFIDENTIALITY NOTICE: This email message, including any attachments, is for the sole use of the intended recipient(s), and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email, and destroy all copies of the original message.
3. Internal email containing PHI within PMC intranet is permissible (from one pacmed.org address to another pacmed.org address).

Protected Health Information (PHI) Facsimile (Fax) Policy

Policy:

PMC will protect the confidentiality and integrity of PHI as required by law, professional ethics and accreditation requirements.

Overview:

1. All PHI received by fax will be handled confidentially.
2. Personnel may transmit PHI by fax when urgently needed for patient care after verification.
3. Routine disclosures of PHI to legitimate users should be made through the Health Data Services Department.
4. Information faxed must be limited to that which is minimally necessary to meet the requestor's needs.
5. PHI not to be faxed or photocopied without a written patient authorization (unless required by law)
 - Behavioral health information
 - Social Work counseling/therapy
 - Domestic violence counseling
 - Sexual assault counseling
 - HIV test results
 - Records related to STDs
 - Alcohol and drug abuse records
6. Fax cover sheets must be used when sending faxes that contain PHI to a new or non-routine recipient. When faxing for a specified, on-demand request, the person transmitting the documents should first call the requestor prior to transmission, and request that the receiver pick up the PHI in a timely manner.
7. After transmission, the user should document what was sent and sign the cover sheet. This is filed in the patient's medical record.
8. Notify the clinic manager of all misdirected faxes.

Notice of Privacy Practices

Policy:

PMC must provide patients with a written notice about its practices related to health information.

Overview:

1. From April 14, 2003 forward all patients will receive a copy of the Notice of Privacy Practices at check in.
2. This information will also be available for viewing in the clinics.
3. The notice is comprised of the following sections: 1. Right to Notice, 2. Distribution of Notice of Privacy Practices, 3. Revisions to Notice of Privacy Practices, 4. Electronic Notices, 5. Joint Notices By Separate Covered Entities, 6. Required Elements of Notice, 7. Documentation of Notice.

Use and Disclosure of Protected Health Information (PHI) for Involvement in Individual's Care and Notification

Policy:

1. PMC may orally disclose PHI to immediate family members and anyone else the individual is known to have a close personal relationship with when the individual provides permission.
2. PMC may use or disclose PHI related to a patient's location, general condition or death to assist with notification of family, personal representative or another person responsible for the care of the individual.
3. When the individual is present, and capable of making health care decision, PMC may use or disclose PHI if:
 - The individual's agreement is obtained or
 - The individual was provided with an opportunity to object and does not do so or
 - It is reasonably inferred, based on professional judgment that the individual does not object to the disclosure.
4. Disclosure of PHI which is directly relevant to a person's involvement in an individual's care will be permitted under the following circumstances:
 - When the opportunity to agree or object cannot be provided either because of incapacity, emergency circumstances or in the absence of the individual and
 - The PMC provider, in their professional judgment, determines that disclosure is in the best interest of the individual
 - In the case of STD, a written Prohibition on Redisclosure statement will accompany the disclosure of the information
5. PMC may use or disclose PHI to a public or private entity authorized by law to assist in disaster relief efforts, to help in the notification to family, personal representative or another person responsible for the care of the individual.

Enforcement, Sanctions, and Penalties for Violations of an Individual's Privacy

Policy:

Violations of PMC Privacy Policies by a workforce member are subject to formal discipline.

Overview:

1. A violation occurs when a workforce member:
 - Accesses, reviews, or discloses a patient's clinical information for any reason not related to their job
 - Discusses with or reveals to any individual(s) clinical information for non-work related purposes or
 - Violates the provisions of the PMC's Privacy Policies
2. Sanctions include
 - First offense and second offense: Depending on the facts may result in oral or written warning
 - Third offense: May result in termination
 - Some offenses may include immediate termination. Intent and severity of offense and consequences will be considered.
 - Disciplinary sanctions will be reported to the appropriate licensing board as required.
3. Other penalties:
 - Legal action by the individual
 - Personal lawsuits according to Washington State law
 - State and Federal criminal investigation and prosecution with substantial fines and prison sentences upon conviction
 - Civil monetary penalties that DHHS may impose

Training

Policy:

PMC has a responsibility to train all workforce members to their responsibilities to protect the confidentiality of an individual's PHI.

Overview:

1. All workforce members will have general awareness training at the beginning of their employment. (The University of Washington HIPAA training residents and fellows complete satisfies this requirement.)
2. Additional training will be provided to each new workforce member on policies and procedures specifically related to their job.
3. PMC will maintain documentation of all training done for all workforce members for 6 years from the date of its creation or the date when it was last in effect, whichever is later.

Verifying Requestors

Policy:

PMC has a responsibility to verify the identity and authority of individuals requesting access to HIPAA.

Overview:

1. Verification Requirements
 - PMC must verify the identity of any individual or organization and their authority for access to PHI if not known to them and obtain any required documentation, statement or representations (oral/written) from the requestor.
 - Verification requirements will be met if professional judgment is used in making a disclosure.
2. Verification Guidelines
 - Best to involve the clinic's Health Data Services Department or clinic director when verifying requestors.