

SUBJECT: CONFIDENTIALITY OF PATIENT INFORMATION
Effective Date: 3/1/84
Revision Date: 5/91, 7/95, 9/96, 3/97, 7/97, 9/98, 3/01, 2/03, 7/03, 8/04, 9/05, 2/07, 1/13/2009
Review Date: 10/13/2010
Approved by: TEC Board of Directors
Rochelle Crollard, Director of Human Resources

POLICY:

It is an expectation of all Clinic staff members to optimize system security and protect patient information. Protected Health Information (PHI) consists of confidential documents stored on the Computerized Medical Record (CMR), Electronic Health Record (EHR), and in the patient's medical record kept for the mutual benefit of the patient, health care professionals, and the Clinic and as such, should be maintained in a confidential manner. PHI includes demographic, patient care and treatment, and financial information about a patient.

No staff member shall access, discuss and/or release confidential information without first obtaining a signed, written authorization by the patient, or by the patient's parent or legal guardian if the patient is a minor (17 years or under or without legal capacity to consent) or incompetent, except as required by law or except as necessary to properly perform assigned job responsibilities. No TEC staff member shall access PHI out of curiosity, for malicious purposes or for personal or malicious financial gain unrelated to Clinic business or for any other non-work related reason.

Staff members who violate these confidentiality requirements are subject to disciplinary action up to and including discharge. Random audits of staff access to the Computerized Medical Record (CMR) are done on a regular basis.

PURPOSE:

To protect patients' right to privacy. To comply with HIPAA Final Privacy Rule (45 CFR 164.501). To protect the Clinic and staff members from legal liability for damages on grounds of defamation or invasion of privacy.

PROCEDURE:

1. Each staff member based on his or her role in The Everett Clinic, is assigned a security level that defines "Minimum Necessary Access". This access, while it does allow the viewing of medical records, mandates the employee views only what is necessary to perform the task at hand. Roles and security levels are assigned at the managerial level based on user profiles created by the HIPAA Oversight Committee.
2. All information relating to a patient's care, treatment, or condition, including dates of service, demographic or financial information as determined by conversation with the patient or information contained in the patient's medical record, the electronic health record, or in the computer system constitutes confidential information and must not be disclosed to unauthorized individuals.
3. Special care must be taken when e-mailing or faxing medical information. In these cases,

patients should be identified through history number or account number only. E-mail should only be used when encryption is available. For further information on faxing, please refer to Clinical Services Policy #318.002, Faxing of Medical Records.

Special care should also be taken when leaving a message on a patient's voice mail or answering machine. Messages should be brief and limited to your name, Clinic/doctor's name (e.g. Snohomish office) and call back number. Appointment reminders should be limited to the doctor's name, Clinic location, date and time of the appointment. **No** medical information including instructions can be left on a message **unless** we have documented permission by the patient to do so in their medical record or the patient has signed a "Friends and Family Consent to Leave Messages" (see Forms on the Intranet). Please refer to the "Standard PEF Flow" as a part of Standard Work for further information (see "Guidelines, Policies and Protocols" on the Intranet).

4. All staff members shall not access and/or release information regarding a patient for personal or non-work related reasons including accessing information about friends, family or spouses. Out of curiosity or concern for a co-worker, friend or family member, a staff member may feel compelled to access or disclose information for personal/non-work related reasons. Such action is considered a violation of this policy. Further, if a staff member receives a request from friends or family for information, he or she should not access or release the information, but refer the requestor to their doctor's office. Exception: Physicians or providers treating their own minor children 12 years of age or under (as in compliance with our policy #127: Guidelines for Release of Medical Information and HIPAA Privacy Standards).
5. When a patient signs a "Consent for Shared Information with Family & Friends" they are granting permission to their health care provider to **verbally** discuss their care with whom they designate or name on the consent form. If a staff member is named by the patient on the consent form, it **does not** also grant or allow the staff member to access or look up the patient's PHI or medical record information. The patient's consent **only** allows the health care provider to verbally discuss the patient's care with whom they designate.
6. Staff members can access their **own** patient information through the CMR, however are encouraged to contact their health care provider. Staff are not permitted and shall not add, delete, amend or edit any information in their medical record including demographic or appointment information. To the extent a staff member believes that PHI in his/her medical record is inaccurate, they can make a written request to the Clinic or specific health care provider to correct or amend the information.
7. A patient's presence in the Clinic (including friends or family members) is considered confidential and should not be disclosed to anyone without proper authorization or permission by the patient. For example, information will not be released to someone calling the Clinic about the presence of a patient. In addition, Clinic staff members are not to disclose the fact that they saw someone they know visiting the Clinic.
8. Staff members must be discreet and aware of their surroundings when discussing patient care or accessing information in the computer during the course of their work, so that information is not overheard or seen by unauthorized individuals or coworkers who are not

involved with that patient's care.

9. Staff members must log off of the computer when away from their desk for any length of time (i.e. breaks, lunch) to prevent unauthorized access to the information or system. Keep your password confidential. Users are responsible for any activity traceable to their individual account/Login ID(s).
10. Managers/Supervisors must fully understand the guidelines for releasing PHI and are responsible for instructing and monitoring their staff regarding the confidentiality of patient information. Staff who are concerned whether a particular release is appropriate should contact their manager or supervisor.
11. A regular, random audit of staff member activity on the CMR is conducted by the Human Resources Department. Unauthorized/suspicious access will be reviewed with the staff member and department supervisor/manager.
12. **Required reporting, investigation and retaliation.** Any staff member who has knowledge of another staff member violating this policy should report this violation immediately to their supervisor/manager, Corporate Compliance Officer, Administration or Human Resources. All reports of alleged breaches of confidentiality or violations of this policy will be promptly investigated. All employees are required to cooperate with such investigations and provide information within their knowledge, when asked to do so. As a part of the Clinic's compliance monitoring or in the course of an investigation, computer reports are generated showing the staff member's activity on the CMR or EHR. Retaliation against any person who reports, in good faith, the alleged violation and/or provides information in connection with any investigation of such report is prohibited.
13. **Violation of policy.** Any staff member who violates the confidentiality of patient information is subject to serious disciplinary action, up to and including termination of employment and may also be held personally liable for their actions. When investigating potential violations of this policy and determining appropriate disciplinary action, TEC will consider three categories* of violations. Categorization of a particular event will be made following an investigation and based on the judgment of the investigating staff.

***All categories will result in disciplinary action up to and including discharge and TEC will retain the discretion to determine the appropriate disciplinary action.**

Category 1 Carelessness: This breach occurs when an individual unintentionally accesses or discloses PHI in violation of TEC's privacy policies. Self-reporting and number of repeated offenses of an unintentional violation will be considered as a mitigating factor in determining appropriate discipline.

Category 2 Curiosity or Concern: This breach occurs when an employee intentionally accesses or discloses PHI in violation of TEC's privacy policies, for purposes unrelated to treatment, payment or operations or any other non-work related reason(s) without malicious intent.

Category 3 Malicious Intent: This breach occurs when a staff member intentionally accesses or discloses PHI with malicious intent or for personal gain.

NOTE: For more detailed and complete information regarding the release of patient information, please contact the Medical Records Department.

Related Clinic policies and forms:

Faxing Medical Records Policy (Clinical Services #318.002)

Guidelines for Release of Medical Information Policy (Admin/Finance #127)

Computer Use Policy (Human Resources #405.001)

Consent to Leave Messages/ Share Information with Family & Friends (see Forms on the Intranet)

Standard PEF Flow (see “Guidelines, Policies and Protocols” on the Intranet).

BREACH OF CONFIDENTIALITY EXAMPLES

Violations of this policy often occur out of curiosity or concern for a friend, acquaintance or family member. These examples show how access to patient information can be used for personal benefit or non-work related reasons. ***Each example is a violation of our policy and would result in disciplinary action including discharge.***

- 1) On her way to a meeting, Lynn passes by the OB/GYN waiting room and sees her neighbor, Julie, being called back into the office by the nurse. That night after work, Lynn tells her husband that Julie must be pregnant because she was at the OB/GYN department today, and thinks they ought to have a shower for her. The next day, Lynn’s husband sees Julie as he’s leaving for work and congratulates her on the pregnancy. Julie gets upset because she isn’t pregnant, and wonders why he would say that.
- 2) Mark and Tina want to have a surprise birthday party for one of their coworkers, Sam, but don’t know his exact birthday. Tina tells Mark that Sam is a patient of the Clinic, and she can look up his birth date on the Plus system. Just out of curiosity, Tina decides to look up his appointment history as well.
- 3) Amy’s coworker and friend, Heidi, had been off work now for almost four days, and wasn’t sure when she’d be back. Amy was very concerned about her friend, and knew she hadn’t been feeling well, but hadn’t gotten many details from Heidi, so looked up her medical record in the CMR to get more information.
- 4) Tara is a new nurse at the clinic who meets “Jim” through an online dating service. On their first date, Jim mentions that he knows the doctor Tara works for, as he had previously gone to him for a procedure. Tara likes Jim, and the next day, Tara accesses Jim’s record on the CMR to check him out a little more thoroughly before she agrees to a second date.
- 5) Janet is a Receptionist at the front desk. She is just finishing a phone call with her mother when a patient walks up to the desk. The patient just happens to be Janet’s brother’s ex-wife. Just before she hangs up, Janet says, “I have to go now, Mom, Rachel is here for an appointment.”
- 6) An employee is a regular customer at Cut N Curl Hair Salon, and apologizes to her hairdresser for being late due to a difficult patient who had some plastic surgery and was not satisfied with the results. The hairdresser remarks that Mary Jones, a regular customer

at the salon, was just in yesterday complaining about services provided to her. The employee confirms that they are talking about the same person and that she is just never satisfied. The hairdresser and employee commiserate about the patient. A neighbor of Mary Jones is sitting in the next chair and overhears the conversation and reports it back to Mary Jones who files a complaint.

- 7) Pam is a Receptionist at the Walk In Clinic. One evening, her mother-in-law comes into the clinic asking to be seen for back pain. When Pam brings up her mother-in-law's name on the computer, a "K" code alerts her to the fact that this patient is a possible drug seeker. The next day, Pam and her husband are at home when his mother calls, saying she is in pain and would he take her to the emergency room. He agrees, but when he hangs up, Pam says "All she wants is to get more pain medication. She's a drug seeker- it says so on her file at the Clinic, so that all the staff and physicians are alerted to it." Her husband is shocked, and when he picks his mother up, confronts her with this information. She is furious, denies being a drug seeker, and calls the Clinic to file a complaint.
- 8) Susan is a newly divorced employee of TEC. She learns that her ex-husband has just started dating a woman who happens to be a patient at the Clinic. Susan is angry that her ex-husband is dating so soon, and decides to look up the woman's medical history on the CMR, to see if she can find any "dirt" on her that she can tell her ex.
- 9) An employee's husband signed the Friends and Family consent form giving permission to his doctor to verbally discuss his care with his wife. The employee went into the CMR and cancelled an appointment for her husband because he was feeling better. While she was in his CMR, she thought she would review the doctor's notes from his last visit, but noticed there was an appointment made for her husband in Behavioral Health the following week. She calls her husband to see why he would be seeing a psychologist.

Important: When a patient signs a "Consent for Shared Information with Family & Friends" they are granting permission to their health care provider to **verbally** discuss their care with whom they designate or name on the consent form. If a staff member is named on the consent form, it **does not** also grant or allow the staff member to access or look up the patient's PHI or medical record information.

- 10) Rita breaks-up with her boyfriend and decides to sue him for the items he took from her house when he left. She knew he had moved out of state and needed his new address to send him the legal papers. When at work the next day, she looks up his new address on the CMR and sends him the required paperwork. The ex-boyfriend calls and files a complaint with TEC accusing Rita of accessing his information without his knowledge or permission. As part of the investigation, computer reports were generated showing Rita's activity on the patient's CMR. We found that Rita had not only accessed his billing information, but also accessed his patient information several times over the last couple of years for non-work related reasons.

Intranet Issues:

- **Author:** Rochelle Crollard
- **Contact:** Carol Felix
- **Reviewed by:** Carol Felix and Rochelle Crollard
- **Key Words for Intranet Search Engine:** privacy, confidential, HIPAA
- **Approval by Various Committees & Dates Approved (if pertinent):**
- **Relevant Departments:**
- **Distributed to: Managers, Supervisors, Staff and Physicians**

PLEASE SEE CONFIDENTIALITY AGREEMENT BELOW.

The Everett Clinic Confidentiality Agreement

As a staff member of The Everett Clinic, and as a condition of my employment, I agree to the following:

1. I understand that I am responsible for complying with The Everett Clinic's (TEC) Confidentiality of Patient Information Policy (#406), which includes complying with HIPAA Privacy Standards.
2. I will treat all information received in the course of my employment with TEC, which relates to the patients of TEC, as confidential and privileged information.
3. I will not access patient information unless I have a need to know this information in order to perform my job.
4. I will not disclose information regarding TEC's patients to any person or entity, other than as necessary to perform my job, and as permitted under TEC's HIPAA policies.
5. I will not access the medical information of my family (including spouse and children), friends, or co-workers Exception: Physicians or providers treating their own minor children 12 years of age or under (as in compliance with our policy #127: Guidelines for Release of Medical Information and HIPAA Privacy Standards).
6. If I receive requests for medical information from my friends or family members, I will not access or release this information and will refer them instead to their doctor's office.
7. I will not log on to or use any of TEC's computer systems that currently exist or may exist in the future using a password other than my own (except as required by Clinitech personnel to perform their job)
8. I will safeguard my computer password and will not post it in a public place.
9. I will not allow anyone, including other staff members (except as required by Clinitech personnel to perform their job), to use my password to log on to the computer.
10. I will log off of the computer whenever I will be away from my desk or work area for any length of time (i.e. breaks, lunch periods).
11. I understand that my activity on the CMR (Computerized Medical Record) is routinely monitored for suspicious, unauthorized and/or unlawful access.
12. I will not take patient information from Clinic Premises in paper or electronic form (including the patient's physical medical record) except as indicated with an approved password protected device. Any paper chart transfers from site to site as necessary for patient care will be done so via a locked courier method and the physical chart will be in the control of the staff member at all times. Remote access to EPHI is allowed by job category as required and only with secure approved communications methods. To the extent that remote access is provided it shall be the responsibility of the staff member to keep all viewing and use of such device secure.
13. I will report violations of this policy immediately to my supervisor, the Corporate Compliance Office and/or Human Resources.
14. Upon termination of employment with TEC, I agree to continue to maintain the confidentiality of any information I learned while a staff member and agree to turn over any keys, access cards, or any other device that would provide access to the Clinic or its information.

I understand that the unauthorized access or disclosure of Protected Health Information (PHI) including medical information, financial information, records and data; or failure to report such or comply with this confidentiality agreement is grounds for disciplinary action, up to and including immediate termination of employment. I acknowledge receiving a copy of The Everett Clinic's Policy and Procedure on the Confidentiality of Patient Information (**revision date 1/13/2009**).

Employee's Signature

Date

Employee's Name (print)

Employee's 4-digit ID #

Please route the signed Agreement to Lynn Thomas, Business Office.