

INSTRUCTIONS FOR GME STUDENTS AND OBSERVERS
**(Medical Students; Medical Fellows; Physician Assistant, Nurse Practitioner,
and ARNP Midwifery students)**

In order to coordinate medical education activities on the medical center campus, the GME office will provide oversight of all learners participating in learning activities at Valley Medical Center (VMC). GME students and observers wishing to participate in a learning experience at VMC are required to complete the attached application and return it with certain documents as outlined in these instructions. Applications and required documents must be returned to the GME office no later than one month prior to the expected start date of the learning session.

Steps for completing the application:

1. The sponsoring provider, who must be a member of the VMC Medical Staff, shall act as the intermediary between the learner and the GME office. The sponsor will be responsible for ensuring the learner completes Section I of the application and reads and signs the Information Privacy Statement (the sponsor will provide a copy of VMC's Confidentiality and Privacy Policy and Information Privacy and Security Standards as noted in the Statement). The application must include a start and end date for the learning session.
2. The sponsor will complete Section II of the application. The educational objective must be outlined in order for the GME office to review and make a decision regarding the learner's ability to participate.
3. Once Sections I and II are completed, the sponsor will return the application with the copies or proof of the following documents to the GME office via fax to (425) 656-5395 or email to familymedicine@valleymed.org:
 - a. Washington State Patrol criminal history background check, performed within the last two years prior to the start of the learning session
 - b. Liability insurance certificate
 - c. Verification of immunizations against measles, mumps, rubella (two doses or positive rubella titer), chicken pox (vaccination or history of), Hepatitis B (for those learners having patient contact), TB screening with PPD within the past year
 - d. Medical License (if applicable)
 - e. Copy of DEA certificate (if applicable)
 - f. Proof of HIPAA training
 - g. Signed Information Privacy Statement
4. Once the application and all required documents are received, the GMEC Chair will review and decide if the learning session is approved. The decision will be rendered in writing by the GMEC Chair by his/her completing Section III of the application and returning a copy to the sponsoring provider.
5. If the session is approved, the GME office will advise IT, Security, and Dictation of learner's name and dates of the learning session, where appropriate. The sponsoring provider will be given contact information for IT, Security and Dictation, as it will be the responsibility of the sponsor and learner to arrange for the needed access with these departments.
6. Any changes to the learning session, including dates, objectives, or sponsoring provider, must be approved in writing by the GMEC Chair.

GME STUDENTS AND OBSERVERS

Valley Medical Center

Section I: This section to be completed by visitor:

Today's Date _____

Full Name _____ Male _____ Female _____

Address: _____

Specialty area and Program: _____

Name of Sponsoring Provider: _____

Learning Session Dates: From _____ to _____
(Month, Day & Year) (Month, Day & Year)

Level of Education: 3rd Year 4th Year (circle one) Other: _____

Name & Address of School or Program _____

Name & Phone No. of Dean/Program Director _____

I hereby certify that the information I submit in this application, including that within any supporting documents, is complete and correct to the best of my knowledge and belief.

Signature of Visitor

Date

.....
Section II: This section to be completed by sponsoring provider:

Type of Learning Session: _____ To observe ONLY – NO HANDS ON
_____ May perform tasks as listed in learning objectives below

Please outline the expected learning objectives below. This section must be completed for all learners, regardless of type of learning session learner will experience.

(continued on next page)

By signing below, the sponsoring provider agrees to the following:

- To conduct departmental orientation, including expectations in HIPAA and universal precautions
- To provide Direct supervision of the learner when in Valley Medical Center
- To obtain patient consent in instances where the learner will have patient contact
- To guide the learning experience to meet the agreed-upon objectives as outlined in this application

Responsible Sponsoring Provider Signature (Primary sponsor, if more than one)

Date

Print Name and contact address, phone number

.....
Section III: This section to be completed by GMEC Chair:

- Approved
- Denied with Reason: _____

Antonio Pedroza, MD - GMEC Chair

Date

.....
Documents list:

1. Instructions for GME Students and Observers
2. GME Visitor and Learner Application
3. Valley Medical Center Information Privacy Statement
4. Valley Medical Center Confidentiality and Privacy Policy
5. Valley Medical Center Information Privacy and Security Standards Policy

INFORMATION PRIVACY STATEMENT

It is the obligation and policy of Valley Medical Center to preserve each patient's and employee's personal and information privacy to the extent specified by law. Non-public information should not be revealed to anyone without proper authorization and need to know as required by Valley Medical Center policy.

I have read and understand the following VMC Administrative Policies:

- VMC's Confidentiality and Privacy Policy
- Information Privacy and Security Standards (Verbal, Paper, PC, Internet, E-mail, Fax & Image, Print, Fiche, Film & Video, Telephone, Voicemail, and Personnel Standards).

As part of my duties I may have access to confidential employee information and Patient Personal Health Information (PHI). It is my responsibility to insure that all PHI and employee information is treated with adequate privacy and security controls.

As part of my job responsibilities I may be assigned computer passwords. I understand that my password will be my electronic signature and my system transactions may be audited at any time. I am held accountable for all transactions committed with my username. I will take "due care" with all types of PHI whether they are verbal, on paper, or in a computer system.

I will access records only on a "need to know" basis to provide treatment, or participate in payment or healthcare operations, or to provide information to someone providing care. In respect to the confidentiality and safeguarding of patient and employee records, ***I will not share my password(s)*** and will log off the system when I have completed reviewing the records.

I understand that any violation of the privacy and/or confidentiality policies and procedures of Valley Medical Center, or state and federal regulations governing the patient's right to privacy or security may result in disciplinary action, up to and including discharge.

Learner's Name: _____

Signature: _____ Date: _____

CONFIDENTIALITY AND PRIVACY CONSIDERATIONS EMPLOYEE RELATIONS WITH PATIENTS

It is inherent in the mission and role of Valley Medical Center that patients will receive considerate and professional treatment at all times including preservation of a patient's reasonable expectations of privacy. As a result each employee must adhere to the following standards:

1. No employee may record, request or use any information concerning a patient's treatment, medical history, insurance status or personal information except with regard to official Medical Center functions.
2. A patient's printed/computerized medical record may only be read and discussed with individuals involved in the patient's treatment/monitoring or those with written or legal authorization.
3. Providing information concerning patients to persons outside of the Medical Center is governed by specific administrative policies. Employees should check these policies or with their supervisors before releasing information to anyone outside of the Medical Center. Generally,
 - The presence of and reason for admission of a patient that has requested confidential status should not be acknowledged.
 - All requests concerning the presence of a patient in the Medical Center and/or reason for admission should be referred to the nursing unit or information desk.
4. When a patient needs or requests a referral to an outside vendor of health care services (e.g. homecare, durable medical equipment, pharmaceuticals etc.) the patient should be told that the Medical Center does not provide such services or products and that the patient may choose any vendor desired. Listing of known available resources may be provided. In no instance may any employee accept any remuneration, directly or indirectly in exchange for referral of a patient to an outside vendor.
5. This policy should be viewed and considered in conjunction with the "Confidentiality and Privacy Considerations: Employee Relations with Patients" policy in the VMC Employment Policy and Procedures Manual available on-line in Valley Times.

USE OF E-MAIL, VOICE MAIL, COMPUTERS AND ELECTRONICALLY STORED COMMUNICATIONS

Valley Medical Center makes a variety of information systems and technical resources available to Employees for the efficient transaction of business, including voice mail, e-mail, Internet access, personal computers, hardware, software and any electronically stored communication ("electronic communication systems"). Electronic communication systems and information systems generally are reserved for the conduct of Medical Center business and may not be used for an Employee's personal business or entertainment during scheduled work time, without specific consent of an Administrator.

Examples of personal or improper use include, but are not limited to:

- ◆ Downloading software or other copyrighted material without complying with licensing agreements and without proper authorization. **THE MEDICAL CENTER DOES NOT CONDONE THE ILLEGAL DUPLICATION OF SOFTWARE AND EMPLOYEES WHO MAKE, ACQUIRE OR USE UNAUTHORIZED COPIES OF COMPUTER SOFTWARE WILL BE SUBJECT TO CORRECTIVE ACTION.**
- ◆ Attempting to access, without proper authorization, VMC's or non-VMC computers and networks
- ◆ Usage for personal business or personal gain
- ◆ Creation of any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin, or disability.
- ◆ Expressing unauthorized personal opinions on behalf of Valley Medical Center in online forums.
- ◆ Soliciting for commercial venture, religious or political causes, outside organizations, or other non-job-related solicitations.
- ◆ Inappropriate purposes, which includes "surfing" for pornographic material

VMC respects the privacy of all Employees. However, Employees who use any of the information systems provided by VMC should understand that VMC does not guarantee the privacy of communications transmitted or stored on information systems.

Although each Employee has individual passwords and access to various information systems, as necessary to perform their duties, any electronic communication system, information system, and any hardware provided by VMC, including personal computers and other items listed above, are VMC property. Likewise, all messages and information composed, stored, sent, or received on these systems are and remain the property of VMC. They are not the private property of any Employee. VMC reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received, stored or sent over electronic communication systems for any purpose. The contents of electronic communications may be disclosed without the permission of the Employee.

Employees should NOT assume that any message transmitted through or stored on electronic communication systems is confidential. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords does not guarantee confidentiality. All passwords and encryption keys must be disclosed to an Employee's Supervisor, Manager or Director upon request.

Notwithstanding VMC's right to retrieve and read any electronic communication, such communications should be respected as private and accessed only by the intended recipient. Employees are not authorized to read, access a file, or retrieve any stored electronic communications that are not sent to them unless it is necessary to carry out their duties for VMC.

Employees are responsible for knowing and following Information Technology Department protocols for using electronic communications systems. Such protocols include: the proper use of systems so as not to cause damage to VMC equipment or software. Examples of improper usage include installing unauthorized software or downloading programs off the internet; the communication of inappropriate information (must adhere to Valley Values and be aligned with Valley business needs).

Employees must strictly comply with Information Technology Department policies and procedures regarding acquiring or upgrading any new electronic communication systems, or adding new functionality to old equipment such as gaining Internet access by way of an existing personal computer. By using information systems at VMC, Employees acknowledge that these systems may be accessed and used by others and consent to VMC's right to access, monitor and disclose contents of such information systems notwithstanding any symbol or other marking designating it to the contrary (such as designating a voicemail as "private" or an e-mail as "confidential").

Any Employee who discovers a violation of this policy shall notify:
networksecurity@valleymed.org.

Any Employee who violates this policy may be subject to corrective action, up to and including discharge.

Employees sign an Information Privacy Statement and are asked to acknowledge this policy in writing but such acknowledgment shall in no way limit the applicability of this policy to all Employees.

This policy should be viewed and considered in conjunction with the "Acceptable Use of Email and Internet for Valley Medical Center Computing Resources" policy in the Administrative Policy Manual available in each department.