UW Medicine
VALLEY
MEDICAL CENTER

INSTRUCTIONS FOR GME STUDENTS
(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. **Also note: this learning experience is not to interfere with any structured learning program already established at Valley Medical Center or any of its campus locations or affiliates, particularly the Valley Family Medicine Residency Program.**

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 or school clinical placement coordinator will be responsible for ensuring the learner completes Section I of the application as well as reading and signing the HIPAA and Privacy Policies (attached). 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. The school may provide written objectives for this section **so long as those objectives clearly define the expected learning experience for this rotation.**

3. Once Sections I and II are completed, the sponsor or school coordinator 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. Signed HIPAA Self Study **OR** the HIPAA Training Certification
    g. Signed Information Privacy, Confidentiality and Information Security Policy

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.

UW Medicine
VALLEY
MEDICAL CENTER

GME STUDENTS

Valley Medical Center

Section I: This section to be completed by visitor:

Today's Date _____

Full Name _____ **Male** _____ **Female** _____

Address/Phone/Email: _____

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)

UW Medicine
VALLEY
MEDICAL CENTER

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**
- **That this learning experience in no way will interfere with any structured learning program already established at Valley Medical Center or any of its campus locations or affiliates, particularly for Valley Family Medicine residents.**

_____ _____

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

_____

Print Name

_____

Contact Address, City

_____

Contact Phone

_____

Contact Email

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

□ Approved

□ Denied with Reason: _____

Comments:

_____

_____

_____

_____

_____ _____

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 HIPAA Self Study**
4. **Valley Medical Center HIPAA Training Certification**
5. **Valley Medical Center Policy on Privacy, Confidentiality and Information Security**

VALLEY
MEDICAL CENTER

Remarkable things happen here.™

Valley Medical Center
Student HIPAA Self-Study

1. Introduction:

Valley Medical Center is committed to protecting patient privacy and maintaining this information securely. Valley Medical Center has compiled this Student Self Study to assist your understanding of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), rules on Privacy, Security, and Transaction Code Sets that became enforceable in April 2003.

The penalties for violating HIPAA can lead to individual or organization fines, jail time, and/or disciplinary action up to and including termination. Additionally, the Department of Justice and the State of Washington have the ability to levy criminal or civil penalties for inappropriate uses or disclosures of patient information.

Valley Medical Center Corporate Compliance and Privacy Office will serve as a resource for HIPAA compliance. You may contact the office at 425-228-3450 or concern_hotline@valleymed.org.

It is essential that everyone who has access to and handles patient information fully understand their responsibility under HIPAA both to avoid personal liability and to protect Valley Medical Center.

2. Relevant Regulations:

The **Privacy Rule** went into effect on April 14, 2003. It established a federal standard of privacy protection for information about patients and defined Protected Health Information (PHI).

PHI includes things such as:

- any information about the patient's physical or psychological condition
- all the information in the patient's medical record
- the patient's name, address, or birth date, social security number, and other personal demographics
- any other information that might reveal something about the patient's situation (for example, the charges on a patient's billing account, the name of the clinic where the patient is being treated, the reason the patient has made an appointment or is in the hospital, etc.)

Such information may exist in written, electronic, oral, or any other form. It is the responsibility of each of us to protect the confidentiality of patient information. The Office of Civil Rights (OCR) oversees and enforces the HIPAA Privacy Rule.

The **Security Rule** went into effect on April 21, 2005, which focuses on keeping patient health information safe, limiting access to health information, and ensuring that information does not go out to the wrong people. Each employee of Valley Medical Center has responsibilities for keeping information secure based upon their specific role(s). To protect the security of patient information, you are asked to follow certain safeguards. The Office of Civil Rights (OCR) oversees and enforces the Security Rule.

The **Employer Identifier Standard** went into effect on July 30, 2002. This portion of the law requires that employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers.

The **Transactions and Code Sets Rule** went into effect in October 2003. This portion of the law directs that claims submissions and other transactions among health care entities be done electronically, according to certain federal standards. The Center for Medicare & Medicaid Services (CMS) oversees and enforces the HIPAA Transactions and Code Sets Rule.

3. Valley Medical Center Privacy Policies:

Valley Medical Center has policies and procedures to facilitate the protection of patient information and compliance with HIPAA regulations and the State of Washington law. HIPAA does not affect state laws that provide additional privacy protections or greater access for patients. The confidentiality protections are cumulative; and when state law requires a certain disclosure -- such as reporting an infectious disease outbreak to the public health authorities -- the federal privacy regulations do not preempt the state law. Appropriate corrective actions will be applied to employees who fail to comply with these policies and procedures. Corrective actions are based upon the relative severity of the violation.

You may view the policies at the following website: http://valleytimes/sites/comppriv/default.aspx

4. Summary of Core Privacy Policies

Every patient who receives care at Valley Medical Center receives our Notice of Privacy Practices. The NOPP explains the rules we follow when using or disclosing patient information.

Valley Medical Center includes all the entities listed within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. Within these entities, patient information may be shared for treatment, payment and health care operations (TPO). Patient information may not be shared with the non-health care components of Valley Medical Center without patient authorization. Valley Medical Center may share patient information with any non-Valley Medical Center health care professional for treatment purposes. That is, to facilitate continuity of care with different health care professionals, those who are involved in treating the patient may communicate about the patient's medical care. When using or disclosing patient information for payment and health care operations, health care professionals may only disclose to non-Valley Medical Center entities the minimum necessary patient information required to accomplish the intended purpose.

Valley Medical Center may not use or disclose patient information to relatives or other persons involved in the treatment or care of the patient, without a verbal or written authorization. When a patient is unable to express his or her wishes, the caregiver should exercise professional judgment on whether or not to release any patient information. If a disclosure occurs under these circumstances, Valley Medical Center will let the patient know of the disclosure as soon as possible.

Valley Medical Center may disclose patient information to a business associate that is performing an activity on its behalf (such as a consultant) when Valley Medical Center obtains satisfactory assurance that the business associate will safeguard the information. Such assurances are documented in writing through a Business Associate Agreement. Relationships between health care professionals involving the treatment of a patient do not require such agreements.

Outside of treatment, payment or healthcare operations, Valley Medical Center may use or disclose patient information without an individual's authorization for the following: (a) public health activities; (b) health oversight activities; (c) specialized government functions; (d) to avert a serious threat to the health or safety of any person; (e) to law enforcement when required to do so by law; and (f) pursuant to the legal process. All other use or disclosure of protected health information must be authorized in writing or verbally by the patient.

Upon admission, patients have the opportunity to decide whether or not to be included in the hospital's inpatient directory. If a patient opts against being included in the directory, Valley Medical Center will not include the patient in the directory, and therefore cannot acknowledge the presence of the patient in response to inquiries.

If a patient opts to be included in the directory, Valley Medical Center may release the condition and location of the patient when an individual asks for the patient by name. With permission of the patient, clergy of the same faith as the patient may be given directory information without asking for a patient by name.

Psychotherapy notes maintained by behavioral health providers are a subset of patient information subject to heightened confidentiality protections. Without the patient's authorization, such notes may **only** be used or disclosed to conduct Valley Medical Center training programs, for treatment by the behavioral health professional, to defend against legal action, to protect the health or safety of any person, or when required by law. If you work or train in an area that might create psychotherapy notes, please ask your manager for more information about the use of psychotherapy notes.

Research involving human subjects (either directly or indirectly through patient information) requires review by an approved Institutional Review Board (IRB). Researchers may use or disclose patient information for research **only** when authorized by the human subject, or pursuant to an IRB-approved waiver of authorization.

As someone who may have direct contact with patients, you should be aware that patients with have certain rights regarding their medical information. These rights, listed in our Notice of Privacy Practices, are generally initiated with the help of the Valley Medical Center Privacy Program. Patients have the right to: (1) request restricted use of their health information; (2) request that Valley Medical Center not disclose their health information to their health plan for those items or services that they pay in full; (3) request Valley Medical Center to contact them in an alternate way; (4) view and receive copies of their health record; (5) request for an amendment (charge or addition) to their record; (6) request for a list of disclosures of their health information; and (7) file a complaint about how Valley Medical Center and individual health care professionals use or disclose their patient information. Valley Medical Center will not retaliate, or tolerate retaliation, against anyone who files a complaint.

5. Your Role in Protecting Patient Privacy

The protection of patient information ultimately depends on the actions of each and every person who has legitimate access to this information. You will likely encounter patient information during your time at Valley Medical Center. Following is a list of the things you as an individual must do to protect patient information: (1) access, provide and use patient information only for job or study-related reasons; (2) access or provide only the minimum information needed; (3) only share/disclose information on a legitimate "need to know" basis; (4) when you must discuss patient information, do so in a private manner or speak softly to lessen the chance that others will overhear; (5) maintain the confidentiality of information to which you are given access privileges; and (6) employees may not access the records of their family members, including minor children, their own, nor any other person if not a job-related duty. This also applies in cases where employees hold authorizations or other legal authority from the patient; (8) secure or log off applications when you leave a workstation; (9) keep printed materials and computer screens containing patient information from public view; (10) dispose and/or shred documents containing patient information properly – in a shredding bin; (11) follow guidelines for using email, fax machines and for leaving patient information; (12) follow guidelines for using email, fax machines and for leaving patient phone messages; and (13) report privacy violations or suspected breaches to your manager or the Valley Medical Center Corporate Compliance and Privacy Office.

6. Valley Medical Center Information Security Policies, Standards & Guidelines

Valley Medical Center has policies, standards, and guidelines to facilitate information security and compliance with HIPAA regulations and Washington State Law. These information security policies apply to any individual who uses a computer connected to Valley Medical Center networks or who has been granted privileges and access to Valley Medical Center computing, network services, applications, and/or resources.

You may view the policies at the following website: http://valleytimes/sites/compriv/default.aspx

Valley Medical Center information security policies and standards impose the following user responsibilities: (1) any individual who uses a computer connected to Valley Medical Center networks or who has been granted privileges and

access to Valley Medical Center computing, network services, applications, and/or resources; (2) must comply with Valley Medical Center policies; (3) must comply with federal and state statutory and regulatory requirements; (4) report all privacy violations to Valley Medical Center Compliance Corporate Compliance and Privacy Office at concern_hotline@valleymed.org or (425) 228-2255; and (5) report all suspected security events and security policy violations to the IT Support/Help Desk x6200.

7. Confidentiality of Information:

- Limit your access, use, and disclosure of patient information to the minimum amount necessary to perform your authorized activity or duty.
- Maintain the confidentiality of all information, including patient information, confidential information, restricted information, and/or proprietary information to which you are given access privileges.
- Use and/or disclose patient, confidential, or restricted information only as allowed by your job duties.
- Discuss patient, confidential, or restricted information in the work place only with those who have a need-to-know and the authority to receive the information.
- Take care to discuss patient, confidential, or restricted information in a private setting and not hold such conversations where they can be overheard by those without a need-to-know.

8. Computer Access Privileges:

- Ensure that your use of Valley Medical Center computers, email, computer accounts, networks, and information accessed, stored, or used on any of these systems is restricted to authorized duties or activities.
- Use your Valley Medical Center email only to conduct work related responsibilities and not forward Valley Medical Center email account or individual business related emails to a non-Valley Medical Center, Valley Medical Center or affiliates email account (e.g. personal email account or other employer provided email account).
- Never electronically access the records of any person if not an assigned or job-related duty.
- Never electronically access the Valley Medical Center records of family members, including minor children, except for assigned job related duties. This also applies in cases where there is an authorization or other legal authority from the patient.
- Protect access to patient and other job-related accounts, privileges, and associated passwords.
- Be accountable for all accesses made under Valley Medical Center login and password and any activities associated with the use of account access privileges.
- Use credentials to access patient accounts and/or systems as provided only for job duties.
- Log out or lock computer sessions prior to leaving the computer.

9. Computer Security:

- Store all patient information, confidential information, restricted information and/or proprietary information on secure servers, encrypted hard drives, or other secure media.
- Never change the computer configuration unless specifically approved to do so.
- Never disable or alter the anti-virus and/or firewall software.

VALLEY
MEDICAL CENTER

Remarkable things happen here.™

Valley Medical Center
Student HIPAA Self-Study
Signature Page

The signature page for the Valley Medical Center HIPAA Student Self-Study is to be removed from the document and turned in to your manager.

Date: _____

Printed Name: _____

Job Title: _____

Signature: _____

Name of Manager: _____

Manager:

File original in departmental personnel file.

VALLEY
MEDICAL CENTER

Remarkable things happen here.™

HIPAA Training Certification

I certify that I have received training on the confidentiality of protected health information, specifically the privacy regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

I understand that I must maintain the confidentiality of individual health care information and agree to comply with Valley Medical Center privacy policies and procedures located at http://valleytimes/sites/compppriv/default.aspx

Additionally I understand and have reviewed and received a copy of the following summary of selected Valley Medical Center Privacy Policy and Procedures:

1. **Policy 1**: Valley Medical Center is health care component of UW Medicine; a complete list of all healthcare components and non-health care components known as "UW Medicine" is listed on Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. Within the entities listed above, protected health information (PHI) may be shared for treatment, payment and health care operations. PHI may not be shared with the non-health care components of the Valley Medical Center without patient authorization unless it is to support the treatment, payment or health care operations of Valley Medical Center.

2. **Policy 2**: Prior to April 14, 2003, and until the individual's first contact with Valley Medical Center for services after that date, Valley Medical Center's entities may continue to rely on the individual's "Registration Consent /Financial Agreement," authorization, or other express legal permission to use and disclose PHI for treatment, payment, health care operations, or other non-research purposes. Each Valley Medical Center entity will obtain the individual's acknowledgement of receipt of the Valley Medical Center Notice of Privacy Practices or make a good faith effort to obtain an acknowledgment for all services provided after April 14, 2003.

3. **Policy 3**: Outlines Valley Medical Center's policy for the administrative requirements related to the Valley Medical Center Corporate Compliance at (425) 228-2255 or concern_hotline@valleymed.org. Administrative requirements include: safeguards (administrative, technical and physical), disclosures by whistleblowers, mitigation, retaliatory acts, waiver of rights, personnel designations, revisions to privacy policies and procedures, and documentation of privacy policies and procedures.

4. **Policy 4**: The law requires Valley Medical Center to train its employees, including physicians, on the organization's policies and procedures about PHI. Valley Medical Center maintains documentation of the training provided to each employee for six years. HIPAA training must be completed within 30 days of hire and appropriate component and job role training including updates when job

responsibilities are impacted because of new or changed policy or procedure within 30 days of the effective date of the change. Each workforce members must sign the Privacy, Confidentiality, and Information Security Agreement upon hire and at each performance evaluation or re¬credentialing.

5. **Policy 5**: Patients and their families have the right to file complaints about how Valley Medical Center and individual health care providers use or disclose their PHI. They may complain to Valley Medical Center Corporate Compliance or the U.S. Department of Health and Human Services Office for Civil Rights (OCR). If any person complains to a member of the Valley Medical Center workforce about a use or disclosure of PHI, the workforce member must contact Valley Medical Center Corporate Compliance immediately. Workforce members are required to cooperate with all compliance investigations. Valley Medical Center will not retaliate, or tolerate retaliation, against anyone who files a good faith complaint.

6. **Policy 6**: The Valley Medical Center corrective action policy requires that appropriate corrective actions be applied to workforce members who fail to comply with privacy and information security policies and procedures. Corrective actions will be based upon Valley Medical Center policies, the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicated a pattern or practice of improper use or disclosure of PHI, and the workforce member's corrective action record. Corrective actions are documented and retained according to Valley Medical Center records retention schedules.

7. **Policy 7**: The policy describes how Valley Medical center may use and disclose PHI for treatment, payment, and health care operations or as required by law. Workforce members must limit their use & disclosure of PHI to the minimum amount of information necessary to perform their authorized activities or duties.

8. **Policy 8**: Valley Medical Center must obtain a valid patient authorization for a disclosure of PHI that is not for treatment, payment or health care operations and within Valley Medical Center. Valley Medical Center may share PHI with any health care professional for treatment purposes without an authorization. Valley Medical Center may share the minimum necessary PHI with non-Valley Medical Center entities for payment purposes. Questions regarding the sharing of PHI for the health care operations of a non-Valley Medical Center entity should be directed to Corporate Compliance. This policy outlines when a patient must sign an authorization for use or disclosure of their PHI, provides the required core elements of an authorization, and describes the patient's right to revoke an authorization.

9. **Policy 9**: Health care professionals may communicate face-to-face with their patients about health related products or services that Valley Medical Center provides. Health care professionals may also communicate with their patients about alternative treatments, coordination of care, or specialty care. Valley Medical Center must obtain the patient's authorization for any use or disclosure of PHI for non face-to-face marketing unless it is a promotional gift of nominal value.

10. **Policy 10**: Regarding fundraising, state law governs because it is more protective of a patient's privacy. Valley Medical Center may use or disclose an approved set of patient demographic

information and the dates of health care services to raise funds for its own benefit. Valley Medical Center must obtain an authorization for the use or disclosure of any other PHI for fundraising purposes. Individuals have the right to opt out of fundraising communications.

11. **Policy 11**: Valley Medical Center has identified staff within Valley Medical Center who will respond to requests for disclosure of PHI. Valley Medical Center verifies the identity of all requestors and the requestors' legal authority for obtaining PHI. Valley Medical Center documents the requestors' authority to receive the PHI prior to release of PHI.

12. **Policy 12**: Valley Medical Center may disclose PHI to an entity ("business associate") that is performing an activity on its behalf when Valley Medical Center establishes the permitted and required uses and disclosures of PHI and obtains satisfactory assurances that the business associate will safeguard the information. Satisfactory assurances are documented in writing through a business associate agreement. Relationships between health care providers regarding the treatment of a patient do not have the same requirements and are therefore not business associate relationships. Please contact Valley Medical Center Corporate Compliance if you have questions about whether a business associate relationship exists in a specific situation.

13. **Policy 13**: Upon admission, patients have the opportunity to decide whether to be included in the hospitals' inpatient directories. If a patient opts out of the directory, Valley Medical Center will not include that patient in the directory. If a patient is incapacitated at admission, the health care professional should exercise his or her best judgment on whether to list the patient in the facility directory until the patient is able to express an opinion. Hospitals may release the condition and location of patients when a person asks for the patient by name. With the permission of the patient, clergy of the same faith may be given directory information without asking for a patient by name. Valley Medical Center may use or disclose PHI to assist in disaster relief efforts.

14. **Policy 14**: With exceptions, the personal representative or legally authorized surrogate decision-maker for the patient may sign the acknowledgement for receipt of the Valley Medical Center Notice of Privacy Practices (NOPP) and make decisions concerning Valley Medical Center's use and disclosure of the adult or emancipated minor patient's PHI. In addition, non-emancipated minors may under certain circumstances acknowledge receipt of the Valley Medical Center NOPP and make decisions concerning Valley Medical Center's use and disclosure of their PHI.

15. **Policy 15**: Provided the patient does not object, Valley Medical Center may use or disclose PHI to relatives or other persons involved in the treatment or care of the patient. If a patient is unable to express his or her wishes, the health care professional exercises professional judgment on whether or not to release any PHI. If PHI is disclosed without the opportunity for the patient to object, Valley Medical Center will let the patient know of the disclosure as soon as possible.

16. **Policy 16 (A-J)**: Valley Medical Center may use or disclose PHI without a patient's authorization in certain circumstances (e.g. public health activities, health oversight activities, and specialized government functions). Valley Medical Center may also use or disclose PHI without a patient's authorization to avert a serious threat to the health or safety of any person, to law enforcement

when required to do so by law, or pursuant to legal process. Please contact Valley Medical Center Corporate Compliance for fact-specific questions.

17. **Policy 17**: Psychotherapy notes maintained by behavioral health providers are a subset of PHI subject to heightened confidentiality protections. Psychotherapy notes may only be used or disclosed absent the patient's authorization to conduct Valley Medical Center training programs, for treatment by the behavioral health professional, to defend against legal action, to protect the health or safety of any person, to a health oversight agency, to a coroner or medical examiner for official duties, or when required by law.

18. **Policy 18**: Research involving human subjects (either directly or indirectly through PHI) requires review by an approved Institutional Review Board (IRB). Researchers may use or disclose PHI for research when authorized by the human subject or pursuant to an IRB-approved waiver.

19. **Policy 19**: Federal law allows Valley Medical Center to use or disclose a "limited data set" for research, public health, or health care operations. A "limited data set" is PHI that excludes 16 specific identifiers of the patient or of the patient's relatives, employers or household members. Valley Medical Center obtains satisfactory assurances through a "data use agreements" from the entity requesting a limited data set prior to allowing the use or disclosure. If PHI is de-identified through removal of 18 specific identifiers, the data is no longer subject to state or federal privacy laws and regulations.

20. **Policy 20**: When using or disclosing PHI for payment and health care operations or when the patient has not authorized the use or disclosure, Valley Medical Center makes reasonable efforts to ensure that the use, disclosure or request of PHI is limited to the minimum necessary PHI required to accomplish the intended purpose. This standard does not apply to disclosures for treatment, to the individual, pursuant to patient authorization or when required by law. For use, Valley Medical Center uses a role-based model to identify appropriate levels of access to PHI. For disclosures made on a routine or recurring basis, Valley Medical Center departments implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

21. **Policy 21**: Valley Medical Center provides all patients (except prisoner patients) a copy of its NOPP, which outlines a patient's rights and describes how a patient's PHI will be used or disclosed. Valley Medical Center is required to make a good faith effort to obtain written acknowledgement of receipt of the NOPP from each patient treated after April 14, 2003.

22. **Policy 22**: Individuals treated at Valley Medical Center facilities have a right to request additional privacy protections, restrictions, and alternative communications regarding their PHI. Valley Medical Center may not be required to agree to a requested restriction. Valley Medical Center will not grant restrictions if continuity of patient care would be impeded. If Valley Medical Center does agree to a restriction, then it will follow the agreed-upon restrictions. All agreed-upon restrictions must be documented in the patient's designated record set. The designated record set contains a patient's medical and billing records, and other information used to make decisions about the patient. When a

patient pays out-of-pocket in full for health care items or services) prior to the service, the patient has the right to restrict Valley Medical Center from disclosing the health care item(s) or service(s) to their health plan.

23. **Policy 23**: A patient has the right to access, inspect or request a copy of PHI contained in the Valley Medical Center designated record set, unless an exemption applies (e.g., psychotherapy notes, information compiled for risk management purposes, etc.). Requests to access, inspect, or photocopy PHI should be referred to Health Information Management. Valley Medical Center employees that have electronic clinical access may use this access to review their medical record on-line. Valley Medical Center employees may not use this access to view the records of their family members or friends.

24. **Policy 24**: A patient may ask a health care professional to correct or amend his or her health care record. Requests must be in writing and state a reason for the requested change. Valley Medical Center has ten days from receipt of the request to respond in writing. If a health care professional receives a request for amendment, he or she must immediately contact the Corporate Compliance and Privacy Office.

25. **Policy 25**: A patient has the right to request Valley Medical Center to provide an accounting of all disclosures from the patient's designated record set, excluding those uses or disclosures for which an accounting is not required (e.g., treatment, payment, or health care operations; uses or disclosures made with patient authorization; or uses or disclosures incidental to an authorized use or disclosure). If you receive a request for an accounting, please contact the Corporate Compliance and Privacy Office..

26. **Policy 26**: A "designated record set" is a group of records consisting of medical and billing records about individuals, information about health plan enrollment, payment, claims adjudication, and case or medical management record systems, and other information used to make decisions about patients.

27. **Policy 27**: Valley Medical Center requires that Social Security Numbers (SSNs) may only be requested in certain business operations, such as when required by law or for operational purposes with appropriate notice of its use and that any system that maintains SSN data must have adequate security controls implemented to protect confidentiality and integrity.

28. **Policy 28**: To protect patient privacy and to decrease the risk of a breach of confidentiality, patient information should only be faxed to fulfill treatment, payment, or health care operations or a specifically authorized request. Fax machines should be safeguarded to reduce the likelihood of inappropriate access to patient information. Requirements for faxing PHI are outlined.

29. **Policy 29**: All Valley Medical Center employees must report breaches of patient information the Valley Medical Center Corporate Compliance and Privacy Office. This policy outlines the process Valley Medical Center follows to notify a patient when their unsecured PHI has been inappropriately accessed or disclosed. The department in which the breach occurs must cooperate with the

investigation, assist in remediating identified issues and may be responsible for funding the response and notification of affected patients.

If I have any questions or would like to know more about these policies and procedures, I can contact the Valley Medical Center Corporate Compliance and Privacy Office or view the materials at http://valleytimes/sites/comppriv/default.aspx

(*Signature page on next page*.)

VALLEY
MEDICAL CENTER

Remarkable things happen here.™

HIPAA Training Certification
Signature Page

I certify that I have received training on the confidentiality of protected health information, specifically the privacy regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") at _____ (name and location of facility) on _____ (day/month/year).

The signature page for the Valley Medical Center HIPAA Training Certification is to be removed from the document and turned in to your manager.

Date: _____

Printed Name: _____

Job Title: _____

Signature: _____

Name of Manager: _____

Manager:

File original in departmental personnel file.

UW Medicine

Non-UW Medicine Workforce Privacy, Confidentiality and Information Security Agreement

Access to UW Medicine Electronic Medical Record (EMR) systems is permitted to authorized users to view protected health information (PHI) electronically. Access is provided only to those individuals whose access has been approved by a UW Medicine Administrator or Director or under a Business Associate Agreement.

A. Non-UW Medicine Workforce Information:

Name _____

Organization _____

Address _____

City, State, ZIP _____

Phone number _____ **Fax:** _____

Email _____

B. Privacy, Confidentiality, and Information Security Acknowledgement

UW Medicine has a legal and ethical responsibility to safeguard the privacy of all patients and protect the confidentiality of their protected health information (PHI). Federal and state laws and regulations govern the privacy of our patients and their health information.

In the execution of services by the organization, I will or may see patients with a variety of medical issues and/or may see and hear confidential information relating to these patients. This relates to information past, present and future physical or mental health or condition of an individual.

As a condition of accessing UW Medicine PHI, I understand and agree that:

- I will comply with federal and state statutory and regulatory requirements (including 45 CFR Parts 160 and 164 (HIPAA) and RCW 70.02).
- I agree to safeguard my UW Medicine access account, and password. I will not share my password with any other person and will not permit others to access the UW Medicine systems through my account. I understand that I will be held accountable for all accesses made under my login and password and any activities associated with the use of my access privileges.
- I will log out or lock computer sessions prior to leaving a computer.
- I understand that I am being given access to PHI and that my access will only occur according to the contract or agreement signed by UW Medicine and the company or healthcare entity I represent or in accordance with my role as a government investigator, auditor or site reviewer. The information disclosed under this agreement will be only used for the purpose(s) described in that contract, agreement or as needed for the investigation, audit or site review.
- I understand that my access will be monitored to assure appropriate use.
    - I understand that the Secretary of the Department of Health and Human Services or the Washington State Attorney General may investigate complaints and may seek criminal prosecution or impose civil monetary penalties to my company and/or me for inappropriate uses or disclosures of certain protected health information.
- I will limit my access, use, and disclosure of patient information to the minimum amount necessary to perform my authorized activity or duty. I understand that the patient information I access is confidential and will not copy or disseminate except as authorized or allowed or required by law. I will only discuss patient, confidential, or restricted information only with those who have a need-to-know and the authority to receive the information.
    - I will keep protected information taken off-site fully secured and in my physical possession during transit, never leaving it unattended or in any mode of transport (even if the mode of transport is locked). I will only take protected information off-site if accessing it remotely is not a viable option.
    - I will store all protected health information on secured systems, encrypted mobile devices, or other secure media.
    - I agree that if I terminate my position with the my company or no longer work in my current position, or otherwise am no longer functioning in the role under which access was granted, I, or my company, will immediately notify UW Medicine IT Services Help Desk at 206-543-7012 or email mcsos@uw.edu and request that my access be deactivated.
- I agree to abide by this agreement and understand that these are privileges granted by UW Medicine to me. I further understand and acknowledge that UW Medicine may terminate this privilege at any time.
    - I will report all concerns about inappropriate access, use or disclosure of protected information, and suspected policy violations to UW Medicine Compliance (206-543-3098 or comply@uw.edu).

_____ _____

Signature **Date**

C. Agreement to be retained by the non-UW Medicine access coordinator

I understand that I will be responsible for this individual when they are accessing PHI and acknowledge that their access to PHI is in compliance with UW Medicine Privacy Policies.

Name: _____ *Signature*_____

Title: _____ *Phone number:* _____ *Date:* _____

Documentation must be maintained for at least six (6) years.