Student Forms Packet

PROVIDENCE Health & Services

Affiliate#:

8	0	0	0	0				

First Name:

M.I.:

Last Name:

Department: Nursing

Position: Student/Faculty

Work Site: OR Region

E-Mail | Print | Reset Form

Student Affiliation Pre -Placement Requirements

Below is the list of requirements that a student needs to meet before beginning their experience with Providence. The table addresses the requirement, how to complete the requirement and where to send the results. For your convenience, we have attached the **Student Forms Packet** containing all the documents referenced in the table.

Requirement	How do I Complete this Requirement	Where do I send the Results
Student Pre-Placement Checklist – This form provides a quick reference of requirements that need to be met.	The checklist needs to be printed, completed and returned as part of the Student Pre-Placement packet.	Include the completed ***Student Pre-Placement Checklist*** with the Student Forms Packet and fax the packet to: **(877) 470-6431**
Background Check – A background investigation must be completed on all students 18 years of age or older who will be placed in a student affiliation assignment with Providence Health & Services – Oregon (PH&S). Background check results must be dated no more than 2 years prior to the commencement of the Student Affiliation Program placement. The background check will include the following checks: 1. **Social Security Number (SSN) Trace Report** – This report lists names and addresses used with the social security number and aides in identifying counties/states of residence. 2. **Office of Inspector General (OIG) Sanctions List and General Services Administration's Excluded Parties Listing System (GSA/EPLS)** – This verification identifies individuals that have been sanctioned by the Department of Health and Human Services (DHHS), Office of Inspector General (OIG) and the General Services Administration's Excluded Parties Listing System (GSA/EPLS) for program related fraud who are ineligible to participate in federally or state funded health care programs. 3. **Criminal History** – Criminal history records must be verified that date back a minimum of 7 years. A conviction is not an automatic bar to employment or to participation in a student affiliation. Each case will be reviewed on an individual basis considering factors such as recentness, seriousness, and nature of the offense as it relates to the position. 4. **Sex Offender Registry** – Reports National Repository of Sex Offender records for all states.	**OPTION 1:** If you do not have a background check dated within the last 2 years and with the required items listed on the left, Providence can initiate a background check through HireRight. Please email us at studentaffiliation@providence.org and we will email you the link to request the background check. Fee: $3y.уЛ (to be paid online to HirewigKt) **OPTION 2:** If you have a background check dated no more than 2 years prior to commencement of placement and it contains the 4 elements listed on the left, include as part of the Student Forms Packet.	**OPTION 1:** Background check results obtained through HireRight will be emailed by the vendor directly to Providence. . **OPTION 2:** Include the ***Background Check Results*** with the completed Student Forms Packet and fax the packet to: **(877) 470-6431**

Requirement	How do I Complete this Requirement	Where do I send the Results
Pre-Placement Drug Screen – ***(Non applicable to contracted high schools through the School Outreach Program)*** The school/student is responsible for ensuring that the student has passed a minimum of a 10-panel drug screen. Specimens received outside this timeframe will not be accepted. Specimen results received from the lab that are "dilute" will not be accepted. Student will be notified that a recollection is necessary. (Recollection fee will be at the student's expense). Student will be responsible for additional fees if drug screen is reviewed by the Medical Review Officer. The 10-panel drug screen must include checks for Alternate Amphetamines, Amphetamines, Cocaine, Opiates, THC, Phencyclidine, Barbiturates, Methadone, Benzodiazepine, Methaqualone, Propoxyphene, Alternate Opiates	**Option 1 – Portland Service Area** ***Legacy Metro Lab*** (multiple location see form) ***Legacy Metro Lab's*** drug screen collection fee is $44.00. Students must present the Legacy Student Affiliate drug screen referral form (included in this packet). Hours vary depending on location. Please refer to referral form for hours & locations. **Option 2 – Outside Portland Service Area** Schools participating outside the Portland Service Area or Oregon Region can partner with a collection facility or research collection sites by logging into http://www.concentra.com or http://www.ushealthworks.com/Home to find a collection facility near their area. If you select **Option 2** – ensure the results are faxed to Providence Regional Employee Health at: ó[illegible]	**Option 1: (Portland Service Area)** ***Legacy Metro Lab*** will fax urine drug screen results ó[illegible]. **Option 2 – Outside Portland Service Area:** Student should instruct the vendor to have drug screen results faxed to Providence Employee Health at: ó[illegible].
Health Screen Verification – School will ensure that students have up-to-date immunizations. Students who will work in at risk departments are strongly encouraged to be protected against Hepatitis B. Students are required to be protected against Measles, Mumps and Rubella (MMR), Varicella (chickenpox), and Tetanus, Diphtheria, and Pertussis (Tdap), and demonstrate either a negative skin test or chest x-ray for Tuberculosis within the last 12 months. Students who will have direct contact with obstetric patients must have documented proof of immunity to Rubella (no declination accepted)	Student will be required to provide the following immunization records upon request by Providence: Hepatitis B: (a) Written documentation of completion of Hepatitis B series or declination statement from Health Care Provider **OR** (b) Laboratory evidence of Hepatitis B status (a positive antibody titer for Hepatitis B) Measles, Mumps, Rubella(MMR) (a) Written documentation of two doses of MMR from Health Care Provider **OR** (b) Laboratory evidence of immunity. (a positive titer for measles, mumps, rubella) Varicella (chickenpox): (a) Written documentation of two doses of Varicella vaccine from Health Care Provider **OR** (b) Laboratory evidence of immunity (a positive titer for Varicella) OR (c) Immune by Disease	Not applicable until requested by Providence as part of the audit process. Once requested, student will need to comply within one (1) business day.

Requirement	How do I Complete this Requirement	Where do I send the Results
	Tuberculosis (TB) (a) Quantiferon Gold TB test **OR** (b) Tuberculin skin testing: If tuberculin skin testing is done, then 2-step TB testing is required. Documentation of a tuberculin skin test within the 12 months prior will be accepted as the initial test of the 2 step test. Influenza vaccine (a) Proof of vaccine for the current year from Health Care Provider or a declination statement. Tetanus, Diphtheria, Pertussis(Tdap) Proof of vaccine from Health Care Provider or other source. (Tdap is recommended for adults over the age of 19 years).	
HIPAA Training – As students will potentially be exposed to medical records and sensitive patient information, it is required that all students receive training in HIPAA (Health Insurance Portability and Accountability Act). School and PH&S are dually responsible for ensuring that students are trained on HIPAA rules and regulations.	Visit the US Department of Health & Human Services site: **Department of Health & Human Services** Review the "Summary of the Privacy Rule" section.	After reading the information, check off the ***HIPAA Training*** requirement on the Student Pre-Placement Checklist.
Non-Employee Acceptable Use and Confidentiality Agreement - Students will potentially be exposed to confidential information related without limitation to patients, customers, members, providers, groups, physician's healthcare information, employee records, and proprietary trade information. It is required that this form be completed as confirmation that the confidentiality of system information will be maintained.	Read attached policies: PROV-PSEC-802 – Acceptable Use of Data and IT Assets Policy. PROV-ICP-716 – Confidentiality Complete and sign the Non-Employee Acceptable Use and Confidentiality Agreement form.	Include the signed ***Non-Employee Acceptable Use and Confidentiality Agreement*** with the completed Student Forms Packet and fax the packet to: **(877) 470-6431**
Acceptable Use Agreement & Code of Conduct Acknowledgement This information describes the appropriate use of Providence information and technology resources including data, systems, networks and devices including but not limited to desktop computers, laptops, PDA's, fax machines and copiers and is intended to promote the confidentiality, integrity, and availability of PH&S information and technology.	1. Review the Code of Conduct booklet which can be found by clicking the link provided below. **Review Code of Conduct** • Click on the link above. • Click on "Code of Conduct" on the left within the site. • View the Providence Code of Conduct at the bottom of the page. 2. Review the Code of Conduct Questions and Answers (FAQ's) in the Student Forms Packet. 3. Read and sign the Acceptable Use Agreement & Code of Conduct Acknowledgement form included in the Student Forms Packet.	Include the signed ***Acceptable Use Agreement & Code of Conduct Acknowledgement*** form with the completed Student Forms Packet and fax the packet to: **(877) 470-6431**

Student Forms Packet (PDF file attached):

- **Student Pre-Placement Checklist**
- **Student Affiliate Drug Screen Referral Form (Portland Service Area-Legacy MetroLab)**
- **Student Affiliate Drug Screen Referral Form (Outside Portland Service area or Oregon Region)**
- **Code of Conduct Questions and Answers for Employees**
- **Acceptable Use Agreement & Code of Conduct Acknowledgement**
- **Non-Employee Acceptable Use and Confidentiality Agreement**
- **PROV-PSEC-802 Policy: Acceptable Use of Data and IT Assets Policy**
- **PROV-ICP-716 Policy: Confidentiality**

Student Forms Packet to be returned to Providence via fax number: (877) 470-6431

- **Student Pre-Placement Checklist**
- **Background Check Results – if not using Option 2 (Hire Right)**
- **Acceptable Use Agreement & Code of Conduct Acknowledgement**
- **Non-Employee Acceptable Use and Confidentiality Agreement**

Should you have any questions about the process, please email us at studentaffiliation@providence.org - You can also reach us by phone at (рло) уфотпсу and ask to speak to thŜ studenű affiliati2n coordinator.

Print Form

Student Pre-Placement Checklist

PROVIDENCE Health & Services

Affiliate#: 8 0 0 0 0

First Name: M.I.:

Last Name:

School:

School Name:

School Coordinator Name:

School Coordinator Email:

Pre-Placement Requirements:

You are required to provide the following items listed below before your assignment begins. Students to check boxes below:

- ☐ Background Check
- ☐ Pre-Placement Drug Screen
- ☐ Health Screen Verification available upon request.
- ☐ HIPAA Training
- ☐ Complete Providence Specific HIPAA education: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
- ☐ Complete a Non-Employee Confidentiality and Non-Disclosure Statement and submit the signed form to Providence Health & Services
- ☐ Complete an Acceptable Use Agreement and Code of Conduct form and submit the signed form to Providence Health & Services

Signatures:

☐ Student has met the Pre-Placement requirements as noted above and is cleared for placement.

Signature of Student: Date (mm/dd/yyyy): / /

Signature of PH&S Designated Representative: Date (mm/dd/yyyy): / /

Please return completed form to: PHSImageNowHRORProvAffiliates@providence.org
(if email from a multfunctional device is not available, fax to (877) 470-6431)

Print Form

Student Drug Screen Referral Form

PROVIDENCE Health & Services

I live:

- ☐ within the... **Portland Service Area or Oregon Region**
- ☐ outside the... **Portland Service Area or Oregon Region**
- ☐ within the... **Medford Service Area**

First Name: _____ M.I.: ____

Last Name: _____

INSTRUCTIONS:

You will need to report your drug screen results from the test required by your school. Typically this is done at program entry. If you do not have the results, you will need to obtain a drug screen prior to any PH&S assignment.

Please use the Legacy MetroLab form for your Drug Test.

☞ Fax Results to Providence Health & Services - Employee Health at (877) 470-6431

☞ Questions about collection? Call (503) 215-6019

SHXHS

Last Modified: Oct. 27th, 2010

Client Services
(503) 413-5295
(800) 950-5295

Legacy MetroLab

DRUG TEST COLLECTION SITE REGISTRATION FORM

Date: _____

Donor: _____ SS#: _____

Company: ***Providence Student Affiliates*** Acct # **17681**

Phone: ***(503) 893-7468*** Contact person referring donor:_____

Self Pay: Drug Test = $44

COMPANY INSTRUCTIONS: Please check appropriate box for purpose of testing and give form to donor.

DONOR INSTRUCTIONS: BRING THIS FORM & PHOTO ID AT THE TIME OF SPECIMEN COLLECTION.

- Avoid drinking excessive amounts of liquids (more than 12 oz) 3-4 hours before specimen collection.
- You may request a drug screen at any of the locations listed below without an appointment.

COLLECTION SITE: Please attach this form to CCF and send to MetroLab – Thank you.

Non-DOT Testing

☐ Pre-Employment ☐ Random

Drug Test Collection Site(s): ◎ **Breath Alcohol testing** ▲ **Saliva Alcohol testing** ☼ **Fast-Trak, 1 Hr Drug Screen**

☐ **Legacy Central Lab**: 1225 NE 2nd Ave. (**at the former Holladay Park Hosp.**), **Portland**, OR 97232
(503) 413-5000 Hours: **M - F** **8:00am - 5:00pm** Fax: (503) 413-5485

☐ **Legacy MetroLab -Tualatin**: 7587 SW Mohawk St, **Tualatin**, OR 97062 ♠◎♦
(503) 692-2700 Hours: M - F 8:30am - 5:00pm Fax: (503) 692-4546
[closed 12 noon – 12:30pm]

☐ ***Legacy MetroLab -Twin Oaks**: 1815 NW 169th Place, Building 6, Suite 6025, **Beaverton**, OR 97006 ♠◎♦
(503) 533-2278 Hours: M - F 8:30am - 5:00pm Fax: (503) 533-8238
[closed 12 noon - 12:30pm]

SHXHS

Peter Barbur - 12/02/2013

Code of Conduct Questions and Answers for Employees

PROVIDENCE Health & Services

System Integrity 2008

Why do we have a code of conduct?

A code of conduct helps identify appropriate behavior and actions in the workplace. The Providence Code of Conduct supports our Mission and values and our commitment to integrity as a Catholic health care and education ministry.

What is a code of conduct?

The Providence Code of Conduct provides us with a set of standards that guides our decision-making and our commitment to "doing the right thing right." This means conducting our business within appropriate ethical, legal and regulatory standards, and complying with Providence's policies and standards.

What is "doing the right thing right?"

In our daily work, doing the right thing right means we:

- dedicate ourselves to Providence's Mission and core values
- uphold ethical principles in the workplace
- follow all applicable laws, regulations, policies and standards governing our business practices
- report concerns about improper, inappropriate or illegal actions promptly, in good faith and without fear of retaliation

Is the Providence Code of Conduct new?

No. The Code of Conduct has been updated to serve as a single resource for all Providence ministries.

Why am I receiving the Code of Conduct in the mail?

Nearly 50,000 people work for Providence. Mailing the updated Code of Conduct to every employee is a way for Providence to demonstrate that we have made the best effort possible to ensure that every employee receives the code. You should receive your copy by mail in **early August.**

What should I do with the Code of Conduct after I receive it?

Please take some time to review the contents. The Code of Conduct is a valuable resource. Keep a copy in your workplace to use as a reference for how to deal with integrity and compliance situations.

What should I do if I have difficulty reading English?

Russian and Spanish translations will be available online for viewing or printing.

Are there other guidelines that may apply to me?

Yes. Additional policies, procedures and standards may apply specifically to where you work and the work you do. If you are unsure what these may be, you should ask your supervisor or manager.

What if I don't work for Providence?

Health care practitioners who are granted privileges at Providence facilities are governed by medical staff by-laws and must follow them. These by-laws provide a process for resolving ethical and compliance issues related to the practice of medicine at Providence. The Code of Conduct provides guidance on the standards expected for everyone who works at a Providence facility.

How will I use the Code of Conduct?

The Providence Code of Conduct asks you to reflect on our Mission and core values as you apply ethical and legal standards to your work. Use it as a resource in the workplace to help you answer these questions:

- Are my actions and decisions consistent with Providence's Mission and core values?
- Am I supporting the spirit, as well as the letter, of laws, regulations, policies or standards?
- Can I explain my actions or decisions without embarrassment to family, friends, co-workers, students or patients?
- Would my behavior harm Providence's reputation in the community or as a ministry focused on health care, education and those in need?
- Who should I contact if I believe a violation has occurred?
- What do I do if retaliation occurs when I raise a concern?
- Who can help me if I still have questions?
- How do I contact my local integrity, compliance and privacy representative?

Do I have any other responsibilities?

Yes, there are seven basic responsibilities:

- Follow the Code of Conduct.
- Perform your job duties in accordance with all federal and state laws or regulations that apply.
- Report all concerns or alleged violations promptly.
- Keep information obtained at Providence confidential.
- Participate in integrity/compliance program training and job-specific compliance education or department training as necessary for your job duties.
- Whenever you are in doubt about something, ask questions.

Will there be a test on the Code of Conduct?

No. In 2009, education about integrity and compliance issues in the workplace will be given to every employee. The Code of Conduct is a part of our integrity program for all Providence ministries.

Subject: Acceptable Use of Information & Information Systems	**Policy Number:** PROV-PSEC-802	
Department: Enterprise Security	☐ New ☒ Revised ☐ Reviewed	**Date:** 1/12/2012
Executive Sponsor: EVP-COO	**Policy Owner:** Chief Information Security Officer	
Approved by: John Koster, MD – President /CEO	**Implementation Date:** 1/15/2007	

Scope: This policy applies to all Providence Health & Services (Providence) workforce members and any other authorized users with access to Providence information and information systems. Access to electronic records by patients, subscribers, and other "consumers" is outside the scope of this policy. This is a management level policy recommended by Leadership Council, approved and signed by the President/CEO.

Purpose: This policy helps Providence protect the confidentiality, integrity and availability of all Providence information systems, and paper and electronic data. The goal of this policy is to describe the appropriate use of Providence information and information systems, including, but not limited to, paper documents, electronic mail, instant messaging, and other web-based technologies (Internet, intranet and extranet).

Definitions: *Confidential Information*, for purposes of this policy, is any information, regardless of format, about patients, employees, students, residents, or business operations that Providence deems should not be available without specific authorization. Loss or inappropriate access to this kind of data could harm patients and Providence's ability to do business. Confidential information includes but is not limited to PHI, ePHI, PII, card holder data (PCI), employee information, financial information and any other information that is intended for limited internal use by Providence.

Other terms are defined in the Providence *Privacy and Security Glossary*.

Policy: Providence information and information systems are intended for Providence business use and must not be used for non-Providence commercial purposes or for purposes that may interfere with the mission of Providence. The electronic transmission of confidential information must adhere to federal and state laws and Providence security, privacy and confidentiality policies and standards. Workforce members and other authorized users shall promote the efficient use of Providence information systems and shall refrain from engaging in activities that interfere with others or disrupt the systems' intended uses. Providence reserves the right to limit or restrict user access to Providence information and information systems.

All Providence information and information systems are the property of Providence. Any use of Providence information and information systems not authorized by Providence is prohibited. The Chief Information Security Officer and Enterprise Security are responsible for the content, communication and enforcement of this policy.

Requirements

A. General requirements for the use of Providence information and information systems

1. Authorized users (including Providence workforce members and other authorized parties) have a responsibility to protect Providence information and information systems. Users shall only access Providence information and information systems for which they are authorized. Misuse of Providence information and information systems may put the organization, data, and patients at risk.

2. Personal use of Providence resources is a limited privilege. Limited personal use of information systems is permitted with the following restrictions: usage must be reasonable, ethical and legal and usage must not interfere with any workforce members' responsibilities or productivity.

3. Prior to accessing Providence information and information systems users are required to acknowledge and agree to follow an Acceptable Use Agreement (Appendix A). Users holding an employment contract or who work through a third-party contract between Providence and the user's third- party employer are required to acknowledge and agree to follow an appropriate acceptable use agreement maintained by EIS Contracting and Procurement. Failure to acknowledge this agreement or violation of this agreement may result in denial of access to Providence information and information systems.

4. Users connecting/synchronizing an approved mobile device to Providence information systems must follow the requirements in the *Device and Media Controls* policy. The mobile device must meet all the required security controls. This applies to all devices whether personally-owned or issued by Providence.

5. Providence reserves the right to monitor all use of Providence information systems and all access to Providence electronic data. Users of Providence information systems have no expectation of privacy with regards to content or use of electronic communications or data within any Providence information system.

6. Providence paper documents, computers, and mobile storage and computing devices must be protected from loss, theft, unauthorized use, disclosure, modification, or destruction. They must be physically secured when taken offsite.

7. All authorized users must take all reasonable steps to protect the privacy and security of confidential patient information. In order to minimize the potential for loss and disclosure, confidential patient information, whether in paper or electronic format, must always be in the possession of the Providence employee or agent, or in a secure location.

8. In accordance with Providence *Early Reporting of Significant Compliance, Risk and Regulatory Issues* policy, all users are obligated to promptly report the loss, theft, unauthorized use, unauthorized disclosure, unauthorized modification or unauthorized destruction of paper documents, computers, or mobile storage and computing devices to Enterprise Security by notifying the Providence Enterprise Information Services Operations Center, or the Providence Integrity Line, or their Information Services Help Desk.

9. All authorized users are obligated to cooperate with Providence investigation or remediation efforts related to information security incidents.

10. All authorized users must follow these and all the requirements of Providence policies. Violation of these requirements may result in disciplinary action up to and including termination of employment or termination of contractual arrangement(s) with Providence. Violations may subject individuals to civil and/or criminal penalties.

B. Terms of Acceptable Use

Acceptable use of Providence information and information systems by authorized users is generally described below:

1. User Access

a. Users are only permitted to use their own Providence- assigned IDs.
b. Users are accountable to protect their unique IDs and passwords.
c. Users may not share their passwords with anyone.
d. Passwords must follow Providence password requirements.
e. Users are not allowed to access Providence information or information systems for which they have not been authorized.
f. The use and handling of mobile storage and computing devices is restricted to those individuals who are authorized to access these devices.
g. Users accessing confidential information (including Protected Health Information) are only authorized to access the minimum information necessary to do their jobs.
h. When accessing Providence confidential information from an off-site location, users must use reasonable safeguards to ensure that the work session cannot be viewed by unauthorized individuals.
i. Users must secure all applications (log out/lock) when leaving a workstation unattended or accessible to unauthorized individuals (e.g., patients, visitors).
j. Users may only use approved remote access services meeting Providence security requirements.
k. Authorized users may not allow any unauthorized user to access Providence information systems or data.

l. Shared workstations (e.g., "auto-login" workstations) may be configured with a unique network identification that is automatically logged on to the Providence network. Access to any confidential information from such shared workstation shall require individual user authentication.

m. Users shall not store confidential information locally on shared workstations.

2. Computing Devices and Software

a. Users may only connect explicitly authorized systems, including mobile storage or computing devices, to Providence networks. Users connecting devices to Providence's network must do so for business purposes only and must be authorized by a Providence Information Services department prior to connecting within the Providence environment.

b. The use of all electronic storage media/portable storage devices must follow Providence *Device and Media Contr*ol policy.

c. Only software and applications authorized by a Providence Information Services department may be installed on a computing system or a mobile computing device.

d. An automobile is not considered a secure location. Under no circumstances should an automobile be used to store confidential information, papers or mobile storage or computing devices, even temporarily.

e. Papers containing confidential information and mobile storage and computing devices shall not be checked with baggage on commercial transportation (e.g., airline, train).

f. Computing devices left unattended in non-Providence locations need to be turned off and be physically secured (e.g., laptop security cable, locked room/drawer).

g. Providence computers must comply with a standard desktop build managed by a Providence Information Services department. This includes but is not limited to the installation of current service packs, current virus protection software, client firewall and firewall configuration, and password protection.

h. Users may not modify the configuration of Providence computers except as authorized by a Providence Information Services department.

i. Computing devices must connect with Providence infrastructure (either locally or remotely) at least monthly in order to receive automated maintenance and inventory services.

3. Confidential Information

a. When electronic confidential information is stored, transported or transmitted outside Providence facilities it must be encrypted.

b. Confidential information may be used, accessed or disclosed only to those who have a need to know. Only the minimal necessary amount of confidential information should be used, accessed or disclosed.

c. Any portable storage or computing device containing Providence confidential information must be encrypted and password protected.

d. Confidential information shall be deleted or removed from the Providence information systems in accordance with the Providence *Records Retention* policy.
e. Providence information classified as confidential or internal use must not be printed at off site locations without management approval.
f. All use of Providence confidential information off-site must follow Providence *Device and Media Controls* policy relating to device and media handling, storage and transport.
g. Paper documents and storage and computing devices containing confidential or internal use information must be secured from unauthorized access or use while awaiting sanitation or destruction and must be destroyed in accordance with Providence *Device and Media Controls* policy.

4. Confidential Patient Information

Authorized users providing patient care in a home setting must secure all confidential patient information by meeting the following requirements:

a. Take only the minimum necessary information for the care of current patients' offsite.
b. Once a patient is no longer under the care of Providence, their confidential information must be deleted from mobile devices and all associated paper documents must be disposed of in accordance with Providence *Device and Media Controls* policy.
c. When involved in patient care in a home setting, confidential patient information must be protected from unauthorized access.
d. Confidential patient information shall not be left in an automobile unattended unless formally authorized by Enterprise Security. When authorized, the laptop must be turned off, hidden, and cable locked to the vehicle.
e. Authorization by a supervisor is required for an employee to store confidential patient information in their home. Authorization is to be based on particular circumstances or a particular job description.
f. Patient confidential information stored temporarily at home must be kept in a secure location such as a locked home, drawer, cupboard or office.

5. Internet Use

a. All use of social media (e.g., social networking) shall be in accordance with Providence *Electronic Social Media* policy.
b. Providence blocks specific categories of inappropriate Internet sites because of information security risks or as requested by leadership. Attempts to access blocked sites are a violation of this policy.
c. Workforce members are subject to Internet filtering and must use approved methods to access the Internet from Providence facilities.
d. Authorized users are responsible to ensure that Internet content accessed via Providence information systems is appropriate for the workplace. Internet access may be limited or disabled at the discretion of Providence.

6. Intranet and Extranet Use

a. Providence intranet, extranet, and other collaborative tools are intended for Providence business purposes only.
b. External parties are not allowed to connect to the Providence intranet unless it is with express permission of Providence. Permission shall be granted via a formal agreement/contract to address specific business needs.
c. Confidential information posted to the intranet or extranet is subject to the requirements of Providence *Confidentiality* policy.
d. Access to the Providence extranet shall only be provided to address particular business needs of external parties and Providence.

7. Electronic Communication

a. Providence regularly monitors electronic communications on its systems including Providence e-mail and instant messaging communications. Sending confidential information through Internet instant messaging is prohibited
b. Users must ensure information contained in all postings, e-mail messages, or any other form of electronic transmission is accurate, appropriate, ethical, truthful, and lawful.
c. Users who have been delegated access to another person's electronic information e.g., e-mail, and calendar, must only access the information when needed.
d. Users may only subscribe to list server discussion groups that are specifically job-related. Legitimate list server subscribers are expected to maintain Providence confidentiality guidelines in all list server discussion correspondence. When participating in list server discussion groups the following disclaimer must be attached to the subscriber's post: *The views and opinions expressed do not necessarily state or reflect those of Providence Health & Services and Providence assumes no liability or responsibility for the accuracy, completeness, or usefulness of the information communicated.*
e. Electronic communications including e-mail can be retrieved regardless of whether the sender and receiver have deleted their copies.
f. User e-mail accounts will be deleted upon notification of termination of employment or contract with Providence. Management may request transfer of mailbox contents prior to termination. Providence may retain mailbox contents as needed.
g. E-mail is a communication tool and is not to be used as a storage mechanism for information. Information subject to specific retention requirements should be stored separately in a suitable electronic or paper system.
h. To prevent viruses, malware and other disruptions to Providence information systems, users shall avoid opening suspicious e-mails and accessing suspicious/inappropriate websites.

8. User-Owned Devices

a. Personally owned devices must meet Providence security requirements and may not connect to Providence information systems or store Providence confidential information unless authorized by a Providence Information Services department.

b. Workforce members will be authorized to connect to Providence systems or networks with an approved PDA/Smartphone device only with management approval.

c. Any approved PDA/Smartphone must support the following security controls before connection to Providence networks is allowed:

1. A Providence device administrator must have the ability to apply appropriate device security controls.
2. A password or PIN must be enforced on the device.
3. Device passwords or PIN must have a minimum length of 4 characters.
4. Data on the device must automatically be erased after 10 failed authentication attempts or the device must lock out further authentication attempts.
5. Devices must be configured to password lock after a maximum of 30 minutes of inactivity.
6. Providence information classified as confidential or internal use shall be encrypted.

d. Providence specifically forbids the transfer of confidential information to user-owned storage or computing devices unless in accordance with Providence policies and control standards.

9. Prohibited Usage

Prohibited communication activities include but are not limited to:

a. Creating or distributing discriminatory, harassing or other threatening messages or images.

b. Creation, storage or distribution of unacceptable content including, but not limited to, sexual comments or images, pornography, racial slurs, hate materials, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

c. Sending chain letters, broadcasting messages unnecessarily, sending messages repeatedly, and excessive or frivolous use of electronic communication technologies.

d. Communicating messages that denigrate, defame, or slander the products or services of Providence or other entities or individuals.

e. E-mailing or otherwise sending confidential information to a personal e-mail account or Internet storage service.

f. Violation of the copyright or trademark law.

g. Violation of confidentiality or non-disclosure agreements.
h. Installation of software not authorized by Providence Information Services departments.
i. Violation of licensing agreements.
j. Gambling, unlawful activity or any activity inconsistent with Providence core values.
k. Representing personal views as those of Providence, including unauthorized use of the Providence logo.
l. Attempting to gain unauthorized access to a computer system of another organization or person.
m. Deliberately jeopardizing the security of any Providence information system.
n. Engaging in any conduct that is contrary to, or inconsistent with, the mission and values of Providence.

Non-Compliance

This policy establishes minimum Providence security specifications. Regional or local procedures or processes may exceed these minimum specifications. Violations of this policy are subject to Providence policy. Any individual who is aware of a violation of this policy is obligated to notify the Enterprise Information Services Operations Center. For circumstances where the requirements of this policy cannot be met, a formal request for an exception must be submitted to Enterprise Security. Enterprise Security will evaluate the risk and potential for compensating security controls (e.g., an "exception" to this requirement). Violation of these requirements may result in disciplinary action up to and including termination of employment or termination of contractual arrangement(s) with Providence. Violations may subject individuals to civil and/or criminal penalties.

Regulatory and Contractual Requirements

The security of confidential information (including electronic Protected Health Information (ePHI) is of particular importance. Violations of provisions of HIPAA can result in employee sanctions (up to, and including, termination of employment), revocation of professional licensure/accreditation, significant civil monetary and/or criminal penalties and damage to Providence's reputation as a responsible leader in healthcare. This policy applies to Providence ePHI as well as, more broadly, to all Providence information. Any references to particular regulatory or contractual requirements (e.g., HIPAA, FDA regulations, state laws, PCI-DSS) are intentionally minimized so as not to indicate that this policy is exclusive to specific categories of information (e.g., ePHI, PII, student records, employee records, genetic information, trade secret information).

References:

PROV-ICP-705: *Corrective Action* – To establish the application of corrective action violations under Providence's Integrity and Compliance Program.

PROV-ICP-717: *Early Reporting of Significant Compliance, Risk and Regulatory Issues* To identify compliance, risk and regulatory incidents that have a significant potential financial, legal, operational and public perception impact for a Providence facility and/or Providence as a whole.

PROV SEC 803: *Device and Media Controls* -- To establish a device and media controls policy for the re-use, storage, transport, tracking and secure destruction of electronic devices, electronic media, and paper.

PROV ICP 715: *Records Retention and Disposal* – To establish requirements for the creation, use, maintenance, retention, preservation and disposition of Providence records.

PROV COMM 604: *Electronic Social Media* – To assure compliance with legal and regulatory restrictions and privacy and confidentiality agreements for social media used for Providence business-related purposes.

PROV-PSEC-806: *Use and disclosures of Protected Health Information Policy* – To outline the requirements for how Providence will comply with the Health Insurance Portability and Accountability Act (HIPAA or Privacy Rule) pertaining to uses and disclosures of protc4ctcd health information (PHI).

PROV-PSEC-811: *Corrective Actions for Privacy and Security Violations* – To define Providence's response to violations for Providence workforce members who fail to comply with state or federal laws or with Providence policies, standards or procedures relating to privacy and security.

PROV-ICP-716: *Confidentiality* – To provide guidance regarding the management, use and disclosure of confidential and proprietary information of Providence.

Privacy and Security Glossary – To ensure consistent use of the terms utilized under the Health Insurance Portability and Accountability Act (HIPAA or Privacy Rule and Security Rule) throughout the Providence Ministry.

Print Form

Affiliate Acceptable Use Agreement and Code of Conduct Acknowledgement

PROVIDENCE Health & Services

Affiliate#: 8 0 0 0 0

First Name: M.I.:

Last Name:

Work Site: OR Region

Position: Student/Faculty

Acceptable Use Agreement:

Compliance with this agreement is a condition of working with PH&S according to policy P-802, Acceptable Use of IT Assets, which can be found at:

http://in.providence.org/sss/resources/documentscentral/policies/Documents/Providence-wide Policies/800 - Privacy and Security/PROV-PSEC-802 - Acceptable Use.pdf

Policy P-802 describes the appropriate use of Providence information and technology resources including data, systems, networks and devices including but not limited to desktop computers, laptops, PDAs fax machines and copiers and is intended to promote and protect the confidentiality, integrity and availability of PH&S information and technology.

I am aware and agree, unless further described herein:

- Internet usage, communications and transactions are not private. All computer activity is recorded and can be traced to specific User ID.
- Information and technology associated with or belonging to PH&S must be protected by taking appropriate measures such as keeping passwords private, encrypting all computers and devices, and locking all portable devices.
- PH&S information and technology is for business use and must not be used for purposes which may interfere or are in conflict with the PH&S mission and/or policies. Any use of PH&S information or technology for a purpose not specifically authorized by PH&S is prohibited.
- PH&S reserves the right to limit or restrict and member's use of information or technology to meet the business and service obligations of the organization.

Although information and technology resources are for business use, limited personal use may be permitted with the following restrictions:

- Usage must be reasonable, lawful and ethical and cannot be offensive or disrespectful to co-workers or others in the work or patient care environment.
- Usage must not interfere or be in conflict with PH&S responsibilities or productivity.

IMPORTANT: In addition to termination, non-compliance could result in further action, including civil or criminal prosecution. Violation of these requirements by a third party contracted with PH&S may result in termination of the representative's contractual arrangement with PH&S for default and may further result in such representative being subject to civil or criminal laws, as applicable.

Code of Conduct Acknowledgement:

I acknowledge that I have received my copy of the Providence Code of Conduct and have had key points explained to me during an orientation training session.

I understand that I am responsible for becoming familiar with the information contained therein; and, that this handbook does not constitute all of the specific policies of Providence.

I further understand that any clarification of the contents of the Code will be provided, upon my request, by my supervisor or a local compliance coordinator or a Region/System Integrity and Compliance Manager.

Affiliate Signature:

By signing this document, I acknowledge that I have read, understand, and agree to abide by the Providence Health & Services Acceptable Use Agreement and the Code of Conduct Acknowledgement. This agreement does not limit my right to use my own general knowledge and experience, whether, or not gained while employed by PH&S, or my right to use information which is known to the general public through no fault of my own.

Signature: _____ Date ____/____/____

Please return completed form to: PHSImageNowHRORProvAffiliates@providence.org
(if email from a multfunctional device is not available, fax to (877) 470-6431)

Subject: Confidentiality	**Policy Number:** PROV-ICP-716	
Department: Integrity, Compliance and Audit Services	☐ New ☒ Revised ☐ Reviewed	**Date:** 6/10/2011
Executive Sponsor: President/CEO	**Policy Owner:** System Director-Integrity, Compliance and Privacy	
Approved by: John Koster, MD - President/CEO	**Implementation Date:** 6/5/2003	

Scope: Applies to all Providence Health & Services ("Providence") employees, members of boards of directors, committee members, members of community ministry boards and committees, and any other person who, as a result of a contractual, employment, volunteer or other relationship with Providence or any of its ministries, has access to confidential and proprietary information of Providence. This is a governance level policy approved by the Board of Directors and signed by the President/CEO.

Purpose: To provide guidance and direction with respect to the management, use and disclosure of confidential and proprietary business, employee, patient, member, student and other information held by Providence and its various ministries. This policy is not intended to restrict employees from discussion, transmission or disclosure of wages, hours and working conditions in accordance with applicable federal and state laws.

Definitions:

Confidential and/or proprietary information for purposes of this policy shall be any information, material, or data that Providence considers and treats as confidential, sensitive or proprietary, and is not in the public domain[1], including, without limitation:

- any medical information[2], also known as protected health information (as defined by HIPAA or other applicable federal or state law), or personally identifiable information held of an individual served by Providence;
- employee/personnel records and information;
- any privileged information from internal/external counsel;
- any board, board committee (at any level of the organization), or medical staff committee minutes, notes or actions;
- nonpublic financial, strategic or operational information; and
- trade-secrets or other confidential information or processes used by Providence in carrying out its activities.

---

[1] Information readily available to public and not subject to any legal restrictions on its use.

[2] Medical information may include the following patient information whether stored externally or on campus and whether electronically stored or transmitted: medical and psychiatric records, including paper printouts, photos, videotapes, diagnostic and therapeutic reports, x-rays, scans, laboratory and pathology samples; patient business records, such as bills for service or insurance information; visual observation of patients receiving medical care or accessing services; verbal information provided by or about a patient.

- any information which Providence or one of its ministries has agreed to keep confidential in accordance with a duly executed confidentiality agreement.

Policy: All persons covered by this policy, (as specified above) shall not purposefully disclose any confidential and/or proprietary information of Providence, unless (i) authorized to do so by Providence; (ii) required to be disclosed to other Providence employees or appropriate workforce members to enable them to fulfill a legitimate job responsibility, provided the individuals receiving the information are advised of the confidential nature of the disclosure; or (iii) required to do so under applicable law.

Requirements: All individuals listed in the Scope section shall act with all reasonable and due care to avoid the inappropriate disclosure of any confidential and/or proprietary information, including assuring that confidential and/or proprietary information is maintained in secure files and locations and securely handled, stored and disposed of; and to avoid its use for any personal gain or the advantage of any outside organizations or entities. Annually, selected covered persons shall be required to execute a statement regarding conflicts of interest and confidentiality. This process is described further in Providence policy PROV-GOV-208. Furthermore, selected covered persons may be required to sign additional and specific confidentiality statements or agreements if they are provided access to particularly sensitive confidential and/or proprietary information.

References:

- PROV-GOV-208 Conflicts of Interest
- PROV-PSEC-801 Information Security Management
- PROV-PSEC-802 Acceptable Use of Data and IT Assets Policy
- PROV-PSEC-811 Corrective Actions for Privacy and Security Violations and PROV- ICP-705 Corrective Actions for Integrity and Compliance Violations

Print Form

Non-Employee Confidentiality and Nondisclosure Statement

PROVIDENCE Health & Services

Affiliate#: 8 0 0 0 0

First Name: M.I.:

Last Name:

Department: Nursing

Position: Student/Faculty

I understand that Providence Health & Services – Oregon ("Providence") is granting me access to systems and information owned or operated by Providence or one of its subsidiaries and I will have access to confidential information not generally available or known to the public, including protected health information. I agree that such information is confidential or proprietary information that belongs to Providence and may only be accessed or used in compliance with applicable law, this agreement and the related agreement between Providence and my employer ("Providence information").

I understand that federal and state laws protect the confidential information to which I will have access and I will abide by those laws. I understand I am required to comply with Providence security policies and standards when utilizing Providence systems and devices or accessing Providence information, including the Providence Acceptable Use of Information & Information Systems (PROV-SEC-802) and Confidentiality (PROV-ICP-716). I understand I am responsible for being familiar with and abiding by these policies and protocols regarding the confidentiality and security of confidential information.

I will not access confidential information for which I have no legitimate need to know nor access my own protected health information. I will hold confidential information in strict confidence and will not disclose or use it except (1) as authorized by Providence; (2) as permitted under written Agreement between Providence and my employer or myself; (3) consistent with the reasons for my access; (4) solely for the benefit of Providence, its patients, its members or other customers; or (5) as required by applicable law.

I understand Providence will issue me an unique user ID and password. I understand that I am not permitted to share this user ID or password with anyone. I agree to notify Providence if I have a reason to believe that any other person may know my user ID or password. I understand my computer account and password will be considered my computer signature, and I will protect it accordingly.

I understand that if I breach the terms of this Acceptable Use and Confidentiality Agreement, applicable Providence privacy and/or security policies, or applicable law (including without limitation the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH), Providence may terminate my access, and Providence will be entitled to all remedies it may have under written agreement or at law, as well as to seek and obtain injunctive and other equitable relief, or contact law enforcement.

AFFILIATE SIGNATURE:

My signature below indicates that I have read, understand, and agree to the above.

Signature: _____ Date ___/___/_____

Please return completed form to: PHSImageNowHRORProvAffiliates@providence.org
(if email from a multfunctional device is not available, fax to (877) 470-6431)