Providence Health & Services - Northwest Washington Region

Non-Employee Confidentiality and Nondisclosure Statement

Name:_____ Date:_____
(*Please Print* – Last Name, First, MI)

I understand that in the course of my employment, I may be granted access to systems or information owned or operated by Providence Health & Services or one of its subsidiaries (PH&S), and will have access to information not generally available or known to the public. I agree that such information is confidential or proprietary information that belongs to PH&S.

Confidential and proprietary information for purposes of this policy shall be as defined in PH&S Confidentiality Policy (PROV-ICP-716). I understand I am required to comply with PH&S security polices and standards when utilizing PH&S systems and devices or accessing PH&S information, including the PH&S Acceptable Use of Data and IT Assets Policy (PROV-SEC-802). I understand my responsibility to become familiar with and abide by applicable PH&S 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. I will hold confidential information in strict confidence and will not disclose or use it except (1) as authorized by PH&S; (2) as permitted under written Agreement between PH&S and my employer or myself; (3) consistent with the scope of services I perform on behalf of PH&S and with applicable PH&S policies and practices; and (4) solely for the benefit of PH&S, its patients, members and other customers.

I understand that this Confidentiality and Nondisclosure Statement does not limit my right to use my own general knowledge and experience, whether or not gained while contracting with PH&S, or my right to use information this is or becomes generally known to the public through no fault of my own.

I understand it is my responsibility to properly use PH&S electronic communication technologies in a manner consistent with PH&S policies, values and applicable laws, all users of PH&S electronic communications technologies must follow the PH&S Electronic Communications Policy (PROV-SEC-812).

I understand that if I breach the terms of this Confidentiality and Nondisclosure Statement, applicable PH&S confidentiality, 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)), PH&S may terminate my association with PH&S, including any written Agreements with PH&S. Further, PH&S 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.

My signature below indicates that I have read and understand the information above.

_____ _____
User's Signature Print Organization/Employer's Name

Subject: Confidentiality **Policy Number:** PROV-ICP-716
Policy Owner: Director-System Integrity **Implementation Date:** 6/5/2003
Date: 6/10/2011

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.
- 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.

Subject: Acceptable Use of Data and IT Assets Policy **Policy Number:** PROV-PSEC-802
Policy Owner: Chief Information Security Officer **Implementation Date:** 1/15/2007
Date: 1/15/2007

Scope: All Providence Health & Services ("Providence") workforce members and any other individual with access to Providence information and/or Providence systems, processes, devices and networks. This is a management level policy recommended by Executive Council, approved and signed by the President/CEO.

Purpose: To describe the appropriate use of organizational assets to promote and protect the confidentiality, integrity and availability of all Providence information classified as confidential and/or internal use and Providence systems, process, devices and networks.

Definitions: None.

Policy: Providence assets are to be used for Providence business. Providence data, systems and devices must not be used for purposes that may interfere with the mission of Providence. Use of Providence data, systems or devices for commercial purposes unrelated to Providence is prohibited. Providence reserves the right to limit or restrict user access to, or use of, Providence data, systems or devices.
Any use of Providence data, systems, or devices 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. This policy supersedes any system or regional information security policies or control standards regardless of department of origin to the extent any such policies or control standards contradict with, or are inconsistent with this policy. This policy establishes minimum Providence specifications. Regional or local procedures or processes may exceed these minimum specifications. Violations of this policy are subject to Providence policy.

Requirements
A. Workforce Members

1. Providence workforce members have a responsibility to protect organizational data, systems and devices. Workforce members are expected to access only Providence information and computing resources for which they are authorized. The misuse of Providence data, systems or devices may put the organization, data and patient care at risk.
2. Although Organizational assets are for Providence business use, limited personal use in accordance with Providence policies and standards is permitted within the following restrictions: usage must be reasonable, ethical and legal and must not interfere with a workforce member's responsibilities or productivity. Personal use of Providence resources is a limited privilege.
3. All Providence workforce members and other individuals with access to Providence systems, data or devices are required to sign an acceptable use agreement. Refusal to sign the agreement may result in denial of access to Providence data, systems and devices.
4. Providence workforce members and any other individuals permitted access to Providence confidential and internal use information and/or Providence systems, processes, facilities, devices and networks shall have an affirmative obligation to immediately notify the Providence Chief Information Security Officer (or his/her designee) and Providence Enterprise Security in the event that an such workforce member or individual has reason to believe that any such Providence information and/or such systems, processes, facilities, devices and/or networks are being improperly used, used in an unauthorized manner, and/or have resulted in an unauthorized or improper disclosure.
5. Providence workforce members who fail to comply with these policy requirements may be subject to disciplinary action up to and including termination of employment. Such actions may be subject to civil or criminal charges, or any combination thereof. Violation of these requirements by a third party contracted with Providence may result in termination of the representative's contractual arrangement with Providence for default and may further result in such representative being subject to civil or criminal laws, as applicable.

B. Non-Workforce Members

1. Non-workforce members with access to Providence data, systems or devices are required to comply with Providence security polices and standards when utilizing Providence systems and devices or accessing Providence information. Non-workforce members agree to comply with the terms of acceptable use listed in this document.

C. Terms of Acceptable Use

1. Acceptable use of Providence information classified as confidential and/or internal use and Providence systems, processes, devices and networks is generally described below:
    a. User Access
        - Users are only permitted to use their own Providence assigned unique ID.
        - Passwords must follow Providence password standards.
        - Users are not allowed to access data, systems, networks or devices for which they have not been authorized.
        - Users accessing patient or confidential data are only authorized to access the minimal necessary data to do their jobs.
    b. Network Authorization
        - Only explicitly authorized systems and devices may be connected to the Providence networks.
        - All wireless devices and networks must be authorized by System Enterprise Security prior to being established within the Providence environment.
        - Only software and applications authorized by Providence Information Services are to be installed on a computing system.
    c. Workstations, Laptops and Mobile and/or Handheld Devices
        - Workstation and laptops must comply with the standard desktop build. Users may not modify the configuration of workstations or laptops.
        - Mobile/handheld computers and devices must be physically protected following Providence requirements.
        - All mobile/handheld devices will employ cryptographic controls.
        - Connection of Providence devices to non-Providence access points must follow control standard 804.007 Mobile and Offsite Computing.
        - Only authorized Providence workforce members or affiliated physicians are permitted to access a Providence device not specifically authorized for public access, and must agree to conform to Providence policy.
    d. Data Storage
        - Electronic transmission of confidential information must adhere to Providence system security standards.
        - Electronic confidential information, both inside or outside of Providence facilities, must be appropriately protected according to control standard 801.006 Cryptographic controls.
    e. Internet Usage. Internet use shall be in accordance with Providence requirements and follow Internet Usage control standard 802.002 Electronic Communications.
    f. Electronic Mail
        - E-mail is to be used for conducting Providence business. Incidental use is permitted as long as it does not interfere with a user's job performance or responsibilities.
        - All e-mails must comply with applicable law.
        - Users of Providence e-mail have no right, nor expectation of privacy. Providence reserves the right to monitor and access any Providence e-mail account.
    g. User Owned Devices. User owned devices may not connect to Providence computers, networks, or systems unless permission has been granted in accordance with approved Providence standards for granting such access.

References: None

Subject: Electronic Communications **Policy Number:** PROV-PSEC-812
Policy Owner: Chief Information Security Officer **Date:** 1/1/2009
Implementation Date: 9/17/2004

Scope: All Providence Health & Services electronic technologies. This is a management level policy recommended by Executive Council, approved and signed by the President/CEO.

Purpose: To define appropriate use of Providence Health & Services (PH&) electronic communication technologies, including but not limited to electronic mail (e-mail), instant messaging and web-based technologies (Internet, Intranet and Extranet).
Definitions: None.

Policy: To ensure PH&S electronic communication technologies are used properly and consistent with PH&S policies, values and applicable laws, all users of PH&S electronic communications technologies must follow this policy. This is a management level policy recommended by Executive Council, approved and signed by the President/CEO.

Requirements:

A. General Electronic Communication Usage

1. PH&S computer systems and the data stored on them are the property of PH&S. Users should have no expectation of privacy and specifically waive any right of privacy with respect to the creation, storage, utilization, receiving and/or transmittal of electronic messages. Users must ensure that information contained in all postings, e-mail messages, or any other form of electronic transmission is accurate, appropriate, ethical, and lawful.
2. Some workforce members are assigned network access accounts and e-mail accounts. Accounts and privileges to additional systems are assigned as necessary for the workforce member to perform their job function. All workforce members are responsible for the use of their individual accounts and their individual passwords. Workforce members are expected to be knowledgeable of these and all policies of Providence Health & Services. Passwords are confidential and shall not be shared with anyone else.
3. Users of electronic communications technologies shall attempt to make each electronic communication truthful and accurate. The same care used when drafting written communication should be used for electronic communication. Care must be taken that information of a confidential or sensitive nature is transmitted appropriately, and to its intended recipient(s).
4. PH&S electronic communication technologies are intended for job-related activities; however, limited personal use is permitted. Personal use is determined as incidental and occasional use of electronic communications technologies for personal activities that should normally be conducted during personal time, such as break periods, or before and after scheduled working hours, and is not in conflict with business requirements of the department.
5. Users shall promote the efficient use of network resources, and shall refrain from engaging in activities that interfere with others or disrupt the intended use of PH&S electronic communication resources.
6. Users are prohibited from the use of PH&S electronic communication technologies for commercial purposes unrelated to PH&S and refrain from the use of e-mail or Web-based technologies for any type of solicitation unrelated to PH&S normal course of business. However, as technology progresses, PH&S and Providence foundations in their sole discretion are given the exclusive right, authority and privilege to solicit charitable donations and or contributions in accordance with our mission, core values and applicable law.
7. Users of electronic communication technologies are responsible for taking reasonable precautions to avoid introducing malicious code into the PH&S network and shall cooperate in efforts to delete or remove any malicious code.
8. Electronic communications will be subject to PROV-ICP-715, Record Retention & Disposal policy and may be deleted or removed from the system in accordance with the records retention schedule.
9. The following are electronic communication behaviors that are prohibited:
    - Creating or redistributing discriminatory, harassing, other threatening messages or images, including hate materials:
    - Examples of unacceptable content include, but are not limited to, sexual comments or images, 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

- Sending chain letters, broadcasting messages unnecessarily, sending messages repeatedly, and excessive or frivolous use of electronic communication technologies.
- Sending or posting messages that defame or slander other individuals or entities
- Violation of the federal copyright law
- Violation of proprietary/trade secrets of PH&S or other organizations
- Sending or posting confidential material or proprietary information outside normal PH&S business activities
- Copying or downloading non-business related software or electronic files without PH&S permission
- Failure to observe licensing agreements
- Sending or posting solicitations or advertisements not related to PH&S business purposes
- Using the Internet for personal political causes
- Sending or posting messages that denigrates PH&S or another organization's products or services
- Representing personal views as those of PH&S in communications
- Attempting to gain unauthorized access to a computer system of another organization or person.
- Engaging in unauthorized transactions that may incur a cost to PH&S or initiate unwanted Internet or e-mail services and transmission
- Deliberately jeopardizing the security of the PH&S computer network
- Any form of gambling
- Engaging in any unlawful activity
- Engaging in any conduct that is contrary to, or inconsistent with, the mission and values of PH&S
- The use of any disk or file encryption, including steganography, not specifically approved by System Information Services
- Any form of pornography
- PH&S logos may not be used to endorse another company

B. Usage Audits of Electronic Communication Technologies

1. PH&S reserves the right to monitor all use regulated by this policy. PH&S management who suspect inappropriate use of electronic communication technologies may request a review of such usage by Enterprise Security. It is the responsibility of PH&S management, in coordination with Human Resources to determine appropriate course of action or disciplinary measures associated with violations of this policy.
2. Internet. PH&S management may request Internet usage reports that show the sites their workforce members did visit or attempted to visit (e.g. blocked sites) through Enterprise Security. PH&S reserves the right to identify users who attempt to access restricted sites and audit the activity of any individual who shows multiple attempts to access sites prohibited by this policy.
3. E-mail or Instant Messaging. PH&S reserves the right to monitor and access workforce members' e-mail or instant message communications when investigating legitimate business concerns or in case of a business emergency. Access to a workforce member's communications is coordinated through Human Resources and Enterprise Security.

C. Electronic Mail Usage

1. E-mail system administrators, during the performance of their duties, may inadvertently see the contents of e-mail messages. Except as provided elsewhere in this policy, they are not permitted to do so intentionally unless necessary for re-routing or disposing of otherwise undeliverable mail, and are not permitted to disclose or otherwise use what they have seen.
2. E-mail system administrators may disclose situations to PH&S management, which may violate the provisions of this policy for the purpose of ensuring ongoing compliance by PH&S users of this policy.
3. Users (e.g. Administrative Assistants) who have access to another person's e-mail and calendar must only access the account when a need to know exists and access only the minimum information necessary.
4. Users should recognize that back-up copies of an e-mail record could exist which can be retrieved regardless of whether the sender and receiver have deleted their copies of it. Such copies are made to protect system reliability and integrity and prevent potential loss of data.
5. Users are prohibited from subscribing to list server discussion groups not specifically job related. Legitimate list server subscribers are expected to maintain PH&S confidentiality guidelines in all list server discussion correspondence. Care must be exercised when participating in on-line discussion groups to ensure that views expressed are not represented as those of PH&S. The following disclaimer must be attached to the subscriber's PH&S e-mail address:

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.

6. External e-mail messages will automatically have attached to the end of the message the standard PH&S footer, detailing that the information is confidential and intended solely for the legitimate use of the intended recipient, and if the message is received in error, any use, copying disseminating or printing is prohibited.
7. User e-mail accounts will be deleted upon notification of termination of employment or contract with PH&S. Management may request transfer of mailbox contents prior to termination or transfer of account outside the PH&S environment in order to transition operations.

D. Electronic Mail Usage with Protected Health Information

1. E-mail containing protected health information (PHI) sent via the Internet must be encrypted. Sending PHI via any instant messaging client is prohibited.
2. Messages with PHI and/or clinical content must be transmitted to only those individuals who have a need to know. Clinical content must be the minimum information necessary.
3. The sending of e-mail messages containing PHI must be transmitted consistent with federal and state law. Generally, the electronic transmissions of highly sensitive information is discouraged unless clinically necessary. Examples of highly sensitive clinical information include: mental health, HIV testing/status, alcohol and chemical dependency, and genetic testing.
4. E-mail is not considered to be a storage mechanism for clinical information.

E. Internet Usage

1. All access to the Internet from PH&S facilities must be done in accordance with PH&S policy. All workforce members must be subject to Internet filtering, with the exception of approved network testing. PH&S explicitly prohibits the viewing and downloading of any pornography.
2. Downloading software from the Internet that is not PH&S business related (e.g. games, screen savers, or executable files) is prohibited. Playing games over the Internet is also prohibited.
3. Unless an Internet resource has been advertised as public, it should not be assumed that it is intended for public areas. Unauthorized access or use of proprietary software or other non-public computing resources may result in civil damages or possible criminal prosecution against the offending person.
4. PH&S is not responsible for material viewed or downloaded by users from the Internet.
5. PH&S utilizes software to identify and block inappropriate Internet sites. Attempts to access blocked sites are in violation of this policy.
6. Accessing the Internet directly, by modem or other means, is prohibited unless the computer is not connected to PH&S network.
7. System Information Services (SIS) may limit or completely disable access to the Internet if such action is in the best interest of PH&S.

F. Intranet Usage

1. PH&S Intranet is intended for Providence business related purposes only. External parties are not allowed to post material to the PH&S Intranet.
2. Users of the Intranet are bound to PH&S confidentiality standards. Proprietary and other information published to the Intranet shall be for PH&S internal use only. It is considered a breach to disclose PH&S confidential or proprietary information discovered through published Intranet content.
3. Personal home page links must not be attached to any PH&S Intranet resource.

G. Extranet Usage

Users of the Extranet are subject to PH&S provisions, safeguards, and prohibitions afforded all PH&S information systems.

H. Appeals Process

Refer to Human Resources polices and procedures for filing an appeal through the established grievance process.

References: None