Current Status: *Active* **PolicyStat ID:** *2310990*

Implementation:	*01/2007*
Last Reviewed:	*01/2016*
Last Revised:	*01/2016*
Next Review:	*12/2017*
Owner:	*Roberto Perez: Director, Security Governance*
Policy Area:	*Privacy and Security*
Department:	
Applicability:	*Providence Health & Services Systemwide*

Acceptable Use of Information & Information Systems, PROV-PSEC-802

Scope:

This policy applies to Providence Health & Services and its Affiliates[1], and their employees, volunteers and others who are in the direct control of Providence (collectively referred to as workforce members) 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, Providence's reputation 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.

Policy:

Providence information and information systems are intended for Providence business use and must not be used for non-Providence personal or 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 Information 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. Providence Information Services may limit the quantity and/or type of personal-use files stored on information systems or networks.
3. Prior to accessing Providence information and information systems users are required to acknowledge and agree to follow an Acceptable Use Agreement (Appendix A or Appendix B). 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 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 an approved mobile device to Providence information systems must follow the requirements in the PROV-PSEC-803 *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 off site.
7. All authorized users must take all reasonable steps to protect the privacy and security of confidential patient and confidential business 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. All users are obligated to promptly report the loss, theft, unauthorized use, unauthorized disclosure, unauthorized modification or unauthorized destruction of paper documents, electronic data, computers, or mobile storage and computing devices to Information Security by notifying the Information Services Operations Center, or the Integrity Line, or the Information Services Help Desk.

9. All authorized users are obligated to cooperate with Providence investigation or remediation efforts related to information security incidents. Questions regarding requests to access specific information or systems as part of a security incident investigation should be directed to the Chief Information Security Officer.
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.
11. Nothing in this policy is intended to restrict employees from discussion, transmission or disclosure of wages, hours and working conditions in accordance with applicable federal and state laws.

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 and must not use the credentials that were assigned to other users.
    b. Users are accountable to protect the confidentiality their unique IDs and passwords.
    c. Users shall not employ the same password used for Providence accounts to access other non-Providence accounts (e.g. personal ISP account, website accounts, etc.).
    d. Users may not share their passwords with anyone.
    e. Passwords must follow Providence password requirements.
    f. Users are not allowed to access Providence information or information systems for which they have not been authorized.
    g. The use and handling of mobile storage and computing devices is restricted to those individuals who are authorized to access these devices.
    h. Users accessing confidential information (including Protected Health Information) are only authorized to access the minimum information necessary to do their jobs.
    i. 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.
    j. Users must secure all applications (log out/lock) when leaving a workstation unattended or accessible to unauthorized individuals (e.g., patients, visitors).
    k. Users may only use approved remote access services meeting Providence security requirements.
    l. Authorized users may not allow any unauthorized user to access Providence information systems or data.
    m. 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.

n. 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 Information Services prior to connecting within the Providence environment.

   b. The use of all electronic storage media/portable storage devices must follow Providence PROV-PSEC-803 *Device and Media Control* policy.

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

   d. An automobile is not considered a secure location and should not be used to store confidential information, papers or mobile computing or storage devices. A mobile computing device should never be left unattended in an automobile. In some circumstances it may be preferable for the user to leave an appropriately secured tablet or laptop computer in a vehicle rather than removing it from the vehicle. Examples of such circumstances include:

      1. The vehicle will only be unoccupied for a few minutes in a well-observed location.
      2. Removing the laptop or tablet from the vehicle will expose the device to more likelihood of loss or theft due to a crowded public venue.
      3. It is infeasible to take the laptop or tablet due to physical constraints.

      In such circumstances, a Providence laptop or tablet may be left in an automobile as long as the following conditions are met:

      1. The device must be stored out out-of-sight (e.g., under a seat or in the trunk).
      2. The vehicle must be locked.

   e. Transportation of Providence computing devices (e.g. laptops, tablets, Smartphones, storage devices) outside of the United States requires approval, and is subject to the following restrictions:

      1. Under no circumstances shall a Providence computing device be transported to a country that has a United States State Department Travel Warning: http://travel.state.gov/content/passports/en/alertswarnings.html
      2. Providence computing devices may be transported to countries not under a State Department Travel warning with the prior approval of the employee's System Director and written approval of an Information Security Officer. Each such request will be evaluated on a case-by-case basis.
      3. Any Providence computing device authorized for transport outside the United States is required to meet the following conditions:

         a. Transport of the device to the foreign country must be required for the conduct of Providence business.

         b. Any required confidential information on the device must be encrypted.

         c. Any non-required confidential information shall be removed from the device prior to travel abroad.

         d. Any inspections, tampering or loss of custody of the device must be immediately

reported to the Enterprise Information Services Operations Center.

e. The device shall not be packed in checked baggage during travel.

f. Return of the device to the United States must be reported to an Information Security Officer within 48 hours of conclusion of travel abroad.

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

g. Under no circumstances are workforce members to use mobile computing devices, moblile phones or pagers while operating a motor vehicle unless such use is hands-free, meets applicable laws and regulations and does not interfere with the safe operation of the vehicle.

h. Providence computers must comply with a standard desktop build managed by Information Services. 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.

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

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

k. Providence Information Services shall maintain an inventory of computer information systems and networks.

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 shall 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 PROV-ICP-715 *Records Retention and Disposal* 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 PROV-PSEC-803 *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 PROV-PSEC-803 *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' located off site.

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 PROV-PSEC-803 *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 Information Security. When authorized, the laptop or tablet must 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 drawer, cupboard or office.

5. **Internet Use**

a. All use of social media (e.g., social networking) shall be in accordance with Providence PROV-COMM-604 *Electronic Social Media* policy.

b. Providence blocks specific categories of inappropriate Internet sites because of information security risks or as requested by leadership.Purposeful attempts to access blocked sites are a violation of this policy.

c. Providence blocks Internet cloud service sites for sharing documents and data. Internet website services or cloud services refer to any resource that is provided over the Internet. Examples of cloud services include, but are not limited to:

1. Any site on the Internet where you are asked to create a user name/password and login.
2. Any site where you are entering patient information through a website form. This includes sites set up by medical device manufactures and medical software companies.
3. Document sharing or note taking sites such as Dropbox, Google docs, and Evernote.

d. Any Non-Providence system that stores Providence data must be approved by Information Security and have an appropriate contract and/or Business Associate Agreement.

e. Workforce members are subject to Internet filtering and must use approved methods to access the Internet from Providence facilities.

f. 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 PROV-ICP-716 *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. Providence workforce members are not permitted to use third-party e-mail providers (e.g., personal e-mail accounts) to conduct Providence business.

   c. 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.

   d. 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.

   e. 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 its Affiliates. Providence assumes no liability or responsibility for the accuracy, completeness, or usefulness of the information communicated.*

   f. Electronic communications including e-mail can be retrieved regardless of whether the sender and receiver have deleted their copies.

   g. 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.

   h. 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.

   i. To prevent viruses, malware and other disruptions to Providence information systems, users shall avoid opening suspicious e-mails and accessing suspicious or inappropriate websites.

8. **Personally-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 Information Services.

   b. Workforce members will be authorized to connect to Providence systems or networks with an approved smartphone, tablet/i-Pad device only with management approval.

   c. Personally-owned devices connecting to the Providence internal network must have current anti-virus installed, a method for receiving periodic operating system and application patches, and secure storage for Providence information.

   d. Personally-owned devices may only be used to access Providence confidential information through approved access methods.

   e. Any approved 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 10 minutes of inactivity.
6. Providence information classified as confidential or internal use shall be encrypted.

f. 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 Information Services.

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 official logo.

l. Attempting to gain unauthorized access to a computer system of another organization or person.

m. Impersonating another person when sending email messages.

n. Deliberately jeopardizing the security of any Providence information system.

o. 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 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 Information Security. Information 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 damage Providence's reputation as a responsible leader in healthcare and result in employee sanctions (up to, and including, termination of employment), revocation of professional licensure/accreditation, significant civil monetary and/or criminal penalties. 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 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 protected health information (PHI).

PROV-HR-422: *Corrective Actions Integrity Compliance Privacy or Security* – To establish Providence's policy and expectations for workforce members who fail to comply with state or federal law or Providence policies and procedures relating to Providence's Integrity, Compliance, Privacy and Security ("ICPS") functions.

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

PROV-PSEC-805: *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.

[1] For purposes of this policy, “Affiliates” is defined as any entity that is wholly owned by Providence Health & Services or Western Health Connect, or is jointly owned by Providence and bears the Providence, Swedish Health Services, Swedish Edmonds or Kadlec name.

All revision dates:	01/2016
Attachments:	A: Acceptable Use B: Acceptable Use