Scope: This policy applies to Providence Health & Services and its Affiliates\(^1\) (collectively known as “Providence”) and their caregivers (employees), employees of affiliated organizations, volunteers and others who are in the direct control of Providence (collectively referred to as workforce members). This is a management level policy approved by the Leadership Council and signed by the President/CEO.

Purpose: To establish requirements for the handling, storage, transport, tracking and secure destruction and sanitation and re-use of computers, mobile storage and computing devices, and paper.

Definitions: For purposes of this policy mobile storage devices are devices designed to store electronic information so it can be easily transported. Mobile storage devices include, but are not limited to media such as tapes, disks, CDs, DVDs, floppy disks, and USB drives (commonly called thumb drives), and portable hard drives. Mobile computing devices have the capability to create, access, transmit, and store data. Mobile computing devices include, but are not limited to laptop computers, tablets, Personal Digital Assistants (PDAs), enhanced cell-phones (commonly called Smartphones), portable medical devices with memory storage such a lab machines, EKG machines, and testing devices used in respiratory therapy.

Other terms are defined in the Providence Privacy and Security Glossary

Policy:
Providence workforce members and any other authorized users who are permitted access to Providence information, systems, facilities, networks or devices shall ensure reasonable safeguards defined in this policy to protect against unauthorized access to Providence information. The Chief Information Security Officer and Enterprise Security are responsible for the content, communication and enforcement of this policy.

Requirements:

1. Providence media and devices must be protected from loss, theft, and unauthorized use, disclosure, modification, or destruction.

\(^1\) For purposes of this policy, “Affiliates” is defined as any entity that is wholly owned or controlled by Providence Health & Services or Western HealthConnect (for example, Swedish Health Services, Swedish Edmonds, Kadlec Regional Medical Center, PacMed Clinics and Inland Northwest Health Services)
2. Providence mobile storage and computing devices shall only be removed from Providence facilities to meet business requirements and will be restricted to those individuals who are authorized to access these devices.

3. Providence specifically forbids the transfer of Providence data to non-Providence owned devices or electronic media unless in accordance with Providence policies. Personally-owned devices may be used (e.g., smartphones, i-Pads, PDAs) if they meet the security requirements established in this policy and are authorized by management and Information Services. See paragraphs 9 and 10 (below).

4. Any computing devices not stored in secured datacenters or server rooms shall protect confidential information by implementing password protection, physically securing the device and having either of the following:

   Encryption of confidential information on the system, or
   
   Technical controls preventing storage of confidential information on the local system (e.g., virtualization or write-prevention).

5. Managers are responsible for ensuring that media and storage devices containing confidential information are turned into Information Services for destruction or sanitization.

6. Mobile storage and computing devices containing confidential information shall be tracked by an inventory management program administered by Information Services.

7. Enterprise Security is responsible for maintaining a list of approved/compatible personally owned devices (PDAs, smartphones, i-Pads, etc.) and operating systems.

8. Management approval is required for workforce members and other authorized users to connect approved devices to Providence systems or networks.

9. Information Services is responsible to develop the following processes and procedures to support the identification, documentation and evaluation of circumstances under which personally owned devices can be authorized to connect to Providence systems or networks:
   
   a. Device registration procedure (inventory and network admission control).
   
   b. Enforcement of appropriate use of the device within Providence and actions to be taken in the event the device is used in a manner inconsistent with Providence security policies or standards.
   
   
   d. Requirement that personally owned devices meet all control standards related to mobile devices.
   
   e. Limitations on the access, processing, storage or transmission of Providence information by the mobile device.
   
   f. Develop and maintain a list of workforce members who are authorized to connect an approved PDA/smartphone, tablet/i-Pad to Providence information systems/networks.
10. Any approved PDA/smartphone, tablet/i-Pad must support the following security controls before connection to Providence networks or information systems is allowed. These requirements apply to personally-owned and Providence owned devices (e.g., smartphones, i-Pads, PDAs).
   a. A Providence device administrator must have the ability to apply appropriate device security controls.
   b. A password or PIN must be enforced on the device.
   c. Device passwords or PIN must have a minimum length of 4 characters.
   d. Providence data on the device must automatically be erased after 10 failed authentication attempts or the device must lock out further authentication attempts.
   e. Device must be configured to password lock after a maximum of 10 minutes of inactivity.
   f. Providence information classified as confidential or internal use shall be encrypted when stored on the device.
   g. In addition to the security controls enforced on the device, users of these devices shall ensure that the transmission of confidential information is protected by encryption; no confidential information may be copied/posted to unapproved 3rd party applications (e.g., Evernote, iCloud, etc.).

11. Department managers are responsible to notify the Information Services Operations Center in the event a PDA/Smartphone device that has connectivity to Providence systems or networks has been used in a manner inconsistent with Providence information security policies or standards. This applies whether the PDA/Smartphone is issued by Providence or is a personally owned device.

12. Biomedical Engineering departments are responsible for ensuring the appropriate labeling, handling, transport, and destruction of medical devices and associated media.

13. Department managers are responsible for the labeling, handling, transport, and destruction of the electronic devices and media used in their department.

14. To prevent unauthorized use or disclosure of information, the following requirements shall be followed for the secure handling, transport, and storage of mobile storage devices:
   a. Chain of custody for Information Assets
      1) Laptops and any other mobile computing or storage devices assigned to the business unit are the responsibility of the business unit manager where the device is being used.
      2) Mobile storage and computing devices containing confidential information must be registered with Information Services and will be reconciled on an annual basis.
3) Mobile storage and computing devices containing confidential information must be inventoried and inventory logs maintained by the department manager. Logs should include:
   a) Name of workforce member assigned
   b) Asset tag number and/or serial number
   c) Date assigned
   d) Date returned

4) Mobile storage and computing devices that are not entered via the inventory procedure and registered with Information Services will be prohibited from connecting to Providence information systems or networks.

b. Media Labeling
   1) Department managers shall identify and appropriately label all mobile storage and computing devices that contain Providence information. Where labeling is infeasible or unwarranted (e.g., due to form-factor or typical use of media) reasonable means must be used to provide some physical identifying characteristic indicating ownership and content (e.g., owner’s name, contact information).

2) Label information may vary. Backup media labels or backup library information should generally include:
   a) classification of the information present on the media
   b) format of the data
   c) software and version used to generate the information
   d) operating system and version
   e) date the media was last created, read and/or checked (for backup media)

c. Device and Media Storage
   1) Department managers shall develop procedures for the secure handling and storage of mobile storage and computing devices for which they are responsible.

   2) Appropriate redundant copies of Providence information stored on mobile storage and computing devices should be maintained to ensure information availability should the device or media be lost, stolen or damaged.

   3) Mobile storage and computing devices must be stored in a location providing physical security appropriate to the media classification level.

   4) Access to mobile storage and computing devices storage must be restricted to enable viewing, handling or use only by authorized individuals.

   5) Information classified as public should be protected to maintain integrity and availability. (For details regarding information classifications see Providence Privacy and Security Glossary.)

d. Media Storage Off-site
   1) Providence information which must be kept long-term shall be stored off-site in an environment providing physical security appropriate to the information classification level.
2) Confidential information that is stored off-site shall be encrypted and password protected.
3) In the event Providence electronic information must be retained for an extended period of time, the data owner shall ensure that both the devices and access technologies (e.g., applications) should be retained. A comprehensive migration strategy should account for vendor stability, system obsolescence and media longevity.
4) Managers responsible for off-site storage shall maintain an inventory for all Providence storage devices stored at the off-site facility.
5) Appropriate privacy / security agreements must be in place with the vendor before the devices or media are transferred to the custody of the vendor. All contracts for off-site media storage will be submitted to EIS Contracting for review and inclusion of appropriate agreements.

e. Media Transport
1) Providence employees or contracted third-party carriers shall be used to transport mobile storage and computing devices containing confidential information, and must protect Providence information from unauthorized disclosure. If the equipment or media is moved from one facility to another, employees or third-party carriers must document chain of custody.
2) Individuals transporting mobile storage devices and mobile computing devices off-site must maintain appropriate physical security of the devices and media during transport.
3) Medical devices being retired or returned to vendor/manufacturer and contain Providence information should have the data irretrievably removed (sanitized) prior to transfer from Providence custody.

15. All Providence business units responsible for disposal of information systems shall develop procedures for the final disposition of all computers, medical devices and mobile storage and computing devices which contain confidential information. Acceptable disposal or sanitization methods will vary depending on the type of computers or devices involved. Sanitation and disposal methods must meet the following requirements:
   a. Devices/Media must be sanitized in a manner which prevents data from being retrieved using file recovery utilities or data scavenging tools (see Appendix A)
   b. Locations performing media/device destruction activities shall ensure that appropriate maintenance programs are followed for equipment used to clear, purge or destroy media
   c. Locations performing media/device destruction activities must have written procedures in place to document processes and procedures for sanitation and destruction
   d. Individuals involved in the sanitization and destruction of devices/media must be properly trained in the use of media sanitation tools, techniques, and procedures
e. Devices/media/papers must be secured from unauthorized access or use while awaiting sanitation or destruction
f. To ensure compliance with Providence destruction requirements, contracted shred and disposal services should have destruction procedures verified as part of the contracting process and periodically thereafter

16. Requirements for Media and Device Reuse:
   a. Media/devices that are to be re-deployed within Providence shall be appropriately sanitized prior to re-deployment. Media sanitation is not generally required for reuse of media in the same environment (e.g., backup tape rotation).
   b. Media/devices that are to be re-deployed outside of Providence must be sanitized (see appendix A) using processes compatible with the storage device being sanitized.
   c. Individuals sanitizing electronic media must document the successful completion of the process to include:
      1) Device Serial Number
      2) Procedure used
      3) Date of sanitization
      4) Name of Individual clearing the device
   d. Devices/media that cannot be completely sanitized (e.g., disks with bad sectors) must be physically destroyed

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 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-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-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.

Appendix A

**GUIDELINES FOR SANITIZATION OF ELECTRONIC STORAGE MEDIA**

<table>
<thead>
<tr>
<th>MEDIA TYPE</th>
<th>DEGAUSS¹</th>
<th>OVERWRITE²</th>
<th>DESTROY³</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnetic Tapes</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hard Disks</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Removable Diskettes</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Optical Disks</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
</tr>
<tr>
<td>CDs/DVDs and Similar Media</td>
<td>N/A</td>
<td>N/A</td>
<td>X</td>
</tr>
</tbody>
</table>

**Processes:**
1. Degauss with a compatible process
2. Securely Overwrite all locations (minimum three times combining pseudorandom pattern and known pattern)
3. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed or grind surface of media to ensure the entire recording surface is removed.

Reference: NIST Special Publication 800-88 *Guidelines for Media Sanitation*