
 <b>HAWAII HEALTH SYSTEMS CORPORATION</b> <i>Quality Healthcare for All</i>  <b>POLICY</b>	<b>Department:</b>  <b>Information Technology Department (ITD)</b>	<b>Policy No.</b>  <b>ITD 0151A</b>
		<b>Supersedes Policy No.</b>  N/A
<b>Subject:</b>  <b>Compliance with Legal Requirements</b>	<b>Approved By:</b>   HHSC Board of Directors By: Donna McCleary, M.D. Its: Secretary/Treasurer	<b>Approved Date:</b>  January 23, 2020
		<b>Last Reviewed:</b>  09/30/19

**I. PURPOSE:**

To ensure compliance with legal and regulatory requirements by all Users and to supplement existing HHSC policies, to the extent such policies do not expressly address relevant legal and regulatory requirements.

**II. DEFINITIONS:**

All capitalized terms not defined herein shall have the meaning set forth in the ITD Glossary. Applicable to all ITD policies and procedures.

**III. POLICY:**

**A. Identification of Applicable Laws and Regulations**

HHSC Corporate and Regional Management shall be cognizant of changes to statutory, regulatory, and contractual requirements affecting Information Assets.

HHSC General Counsel, Corporate and Regional Compliance Officers, and the CISO shall monitor all applicable news and informational sources, e.g., public announcements, professional organizations, etc., for news of proposed or pending statutory and/or regulatory changes that may require changes in the business processes used to safeguard and protect HHSC information and Information Assets, including ePHI.

The Privacy and Security Council (CMP 0021A Privacy and Security Council policy) shall review proposed or pending changes in statutory and/or regulatory requirements and, to the extent necessary, recommend amendments to current information security policies, standards, and procedures.

All new contractual requirements promulgated by federal or state law or regulation that pertain to safeguarding Information Assets shall be brought to the attention of the CISO who shall evaluate the requirements and, if needed or appropriate, submit the information and any relevant recommendations to the Privacy and Security Council for action.

## **B. Intellectual Property Rights**

### **1. Software Licenses**

Installation of unlicensed commercial (off-the-shelf) or proprietary Software on servers, personal computers, laptops, appliances, or other computing devices owned by HHSC is a violation of HHSC information security policy and, possibly, copyright law. Workforce members may be subject to disciplinary action up to and including termination, subject to applicable collective bargaining agreements.

Users may be required to show proof of the license status for Software installed on issued Information Assets assigned to User to validate the legal use of the Software. Such proof shall be demonstrated by providing copies of the original purchase orders, receipts, license keys, labeled, and serialized distribution media, or other appropriate means with sufficient specificity to reasonably conclude valid license status.

Downloaded Software shall come from a known, reputable source, and User shall retain evidence that the Software is properly licensed or obtained under a legitimate open-source license agreement.

License documentation for shared Workstations in public areas with a standardized configuration shall be maintained by ITD.

### **2. Other Downloaded Materials**

Commercial recordings (video, audio) or other copyrighted material shall be:

- Obtained legally with proof of ownership available on request
- Used in compliance with the license agreement associated with the materials, which may include limiting the right to make copies and restricting the use of the materials to specific devices, Workstations, etc.

### **3. Education and Enforcement**

The CISO shall include, among other topics, intellectual property rights awareness in the information security training program.

The CIO shall develop and maintain a procedure for auditing compliance with this policy. This shall include, but not be limited to:

- Use of automated inventory tools
- Random spot checks performed as part of a periodic security assessment by the IST.
- Random audit of devices under repair by the TSD and Regional End User Support Teams.

## **C. Protection of Organizational Records**

CMP 0008A, Retention of Records policy, defines minimum information retention periods. Where there are varying retention periods or where it is technically or economically not feasible to separate information with different retention periods, the longest retention period shall take precedence.

When the retention period is not specified in CMP 008A Retention of Records policy, or where it is not clear, the Information Owner shall expressly specify in writing the required retention period, which shall be maintained in the inventory of Information Assets as described in ITD 0113A, User Responsibility.

Information that is essential for normal HHSC operations shall be backed up consistent with the requirements defined by the Information Owner, as set forth in ITD 0113A User Responsibilities Policy and ITD 0105A Backup policy. Any removable media shall be stored in accordance with the manufacturer's recommendations. During the retention period, information shall be preserved in a manner that decreases the potential deterioration of the media.

## **D. Information Protection and Privacy of Personally Identifiable Information**

### **1. Disclosure of Confidential-Reportable Information**

Personally Identifiable Information (PII) is classified as confidential-reportable and shall be secured pursuant to the provisions set forth in ITD 0009, Data Classification policy. PII includes, but is not limited to, information that is protected by federal and state laws and regulations.

For additional information, please refer to HIPAA and other related privacy policies located on the HHSC intranet under Corporate Compliance. These policies address, among other topics, special requirements concerning the release of certain alcohol and drug abuse treatment records and psychotherapy notes.

### **2. Privacy Expectations of Information Stored On Information Assets**

HHSC-issued laptops, PCs, "smart phones," or other computing devices, along with the programs and files that they contain, and the networks and systems (i.e., file, e-mail, database servers, etc.) to which they connect to or use for storage, are the property of HHSC.

HHSC reserves the right to review, audit, intercept, copy and disclose any files, activity logs, or programs contained on any Information Asset, including HHSC issued PCs, laptops, file servers, e-mail servers, etc. without notification to or requesting permission from the User, Information Owner, or creator of the information or files.

- Such access shall take place in the course of performing corrective or preventative maintenance.
- For investigative or business continuity purposes, access shall be initiated by a written request up through the relevant chain of command to the CISO, and shall, to the extent deemed necessary by CIO, involve the designated HR representative for the Workforce member's department.
- E-mail that triggers IDS alerts may be reviewed, without notice to the recipient, prior to delivery to the User.

### **3. Privacy of Personal Information**

Disclosure of personal information that is not classified as confidential-reportable related to a Workforce member to external parties shall not occur unless expressly permitted or

required by law, or consented to in writing by the Workforce member whose information is being disclosed in writing.

#### **4. Electronic Monitoring Areas**

Users shall be subject to electronic monitoring while in Secure Areas, including data centers, communication rooms, and other areas where critical Information Assets have been deployed.

### **E. Prevention of Misuse of Information Processing Facilities**

#### **1. Use of HHSC Equipment**

Computers, Hardware, Software, and networks purchased by HHSC are the property of HHSC. HHSC may assign one or more PC, laptop, tablet, cellular phone, "smart phone" or similar personal computing devices to a User. There shall be no presumption of exclusivity or entitlement inferred by such an assignment. Any such HHSC device shall be reclaimed for other purposes, reassigned to another HHSC User or Workforce, or it may be retired at any time based on operational needs.

Any User engaged in unauthorized activities, including those addressed in ITD 0051A, Information Security policy, including the Workforce Accountability and Responsibility provisions, shall be subject to corrective action, including up to termination of employment in accordance with collective bargaining agreements, if any, and HR Guidelines.

#### **2. Internet Use**

Access to the Internet shall be for the sole purpose of supporting HHSC business processes, mission, and goals consistent with ITD 0005A, Information Systems Access policy.

The following provisions shall apply to Internet use:

- Access to the Internet shall be in compliance with applicable statutes, regulations and HHSC policies, including those that prohibit harassment and discrimination in the workplace. In addition, Users are expected to apply common sense and judgment to avoid any communication that is disrespectful, offensive, or illegal.
- Access to the Internet from Workstations within the HHSC network shall be allowed only through a HHSC firewall.
- Monitoring and filtering of Internet activity shall be conducted to protect the security and availability of Internet services within the HHSC network. Monitoring of Internet usage may performed at any time and without prior announcement. See ITD 0109A Monitoring policy.
- The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics or other materials obtained from the Internet shall be done only with the permission of their authors/owners. It shall be assumed that all materials on the Internet are copyrighted unless expressly provided otherwise.

#### **3. E-mail Use**

HHSC provides access to the enterprise e-mail system for the sole purpose of supporting HHSC business processes, mission, and goals. E-mail is only to be used as a business

tool to facilitate communication and information exchange required by users of the HHSC enterprise e-mail system.

The following provisions shall apply to e-mail use. This list is not exhaustive, and other provisions shall be applied in accordance with future business use or statutory requirements. The enterprise e-mail system is owned by and maintained by HHSC to satisfy its business needs. Therefore all e-mail messages stored on the enterprise e-mail system is the property of HHSC. To maintain security of the HHSC network, only the following types of e-mail accounts are approved for use:

- HHSC e-mail system accounts;
- Business related external web-based e-mail accounts approved by department managers and ITD;
- Web-based and third-party ISP e-mail accounts shall not be accessed through the HHSC network, except where approved by the CISO for business purposes, and documented as an Information Security Policy Exemption Request;
- Automatic forwarding of enterprise e-mail system account messages to any external e-mail account is prohibited;
- Enterprise e-mail system accounts may be accessed by System Administrators to maintain the integrity and security of the enterprise e-mail system;
- E-mail messages that contain ePHI and other confidential information shall not be sent to recipients outside of the enterprise e-mail system unless encrypted by HHSC approved encryption methods. Prohibited e-mail content practices include, but are not limited to sending:
  - chain-letter messages;
  - discriminatory, obscene, derogatory, defamatory, or any other types of inappropriate messages;
  - messages that contain sexually explicit material;
  - messages that contain ethnic or racial slurs, or any words or images that could be interpreted as disparaging of others based on race, color, ancestry, national origin, marital status, gender identity or expression, sexual orientation, age, disability, religion, or English proficiency.
- To enforce prohibited e-mail content compliance, HHSC Corporate and Regional Executive Leadership reserve the right to approve monitoring of User e-mail messages.

#### **4. Instant-Messaging Use**

Use of free instant-messaging services is prohibited unless expressly approved by ITD and subject to the adoption of a system wide policy.

#### **5. Text-Messaging Use**

Use of text-messaging services shall be the subject of a system-wide policy and approved by ITD. Any such text-messaging services used to exchange HHSC business- or patient-related information shall provide encryption-in-transit, encryption-at-rest, and adequate logging of text-messages.

## **F. Regulation of Cryptographic Controls**

Any computer Hardware or Software that is produced by HHSC shall comply with current federal statutes regulating the export of cryptographic technology.

## **G. Protection of Information for Legal Processes**

Upon the issuance by the HHSC General Counsel of a "litigation hold" on data or information, the CIO or designee shall notify the appropriate System Administrators, Information Owners, and/or IST, and provide instructions to take necessary measures to preserve and collect the required data and information.

Whenever evidence clearly shows that HHSC is the victim of a computer or communications crime, a thorough investigation shall be performed by ITD Security Incident Response Team (SIRT). This investigation shall provide sufficient information for HHSC Corporate and Regional Management to implement procedures to ensure that (1) such incidents are not likely to re-occur, and (2) effective security measures have been re-established.

### **1. Sources of Digital Evidence**

For every production computer system, the IST and/or System Administrators shall identify the sources of digital evidence (the information) that reasonably could be expected to be used in a legal matter or requested by the HHSC General Counsel for litigation holds. These sources of evidence shall then be subject to a standardized capture and retention process comparable to that used for vital records. Under no circumstances shall information that is the subject of a litigation hold be destroyed unless the HHSC General Counsel or designee issues written notice that the litigation hold has been lifted and that information may be destroyed consistent with the HHSC Retention of Records policy.

### **2. Disclosure of Information to Law Enforcement**

By making use of Information Systems, Users consent to allow all information stored on the network to be divulged to law enforcement. HHSC Corporate and Regional Management, after receipt of advice from the HHSC General Counsel or designee, reserves the right to determine what information shall be divulged to law enforcement about Users of HHSC Information Systems. Information shall be divulged if HHSC Corporate and Regional Management, after receipt of advice from the HHSC General Counsel or designee, finds it reasonably necessary to:

- (a) Satisfy any applicable law, regulation, legal process, or enforceable governmental request;
- (b) Enforce security policies, including investigation of potential violations thereof;
- (c) Detect, prevent, or otherwise address fraud, security or technical issues; or (d) Protect against imminent harm to the rights, property or safety of HHSC, its Users or the public as required or permitted by law.

All disclosure of information to law enforcement shall be coordinated through HHSC General Counsel and Facilities' security departments.

### **3. Internal Investigations**

Until charges are pressed or corrective action taken, all internal investigations of alleged criminal or abusive conduct shall be kept strictly confidential to respect and preserve the reputation of the suspected party.

### **4. Forensic Analysis Process**

Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computing crime or fraud and abuse trial, shall be performed with a copy rather than the original version.

### **5. Information Security Investigations**

All HHSC internal investigations of information security incidents, violations, and problems, shall be conducted by trained staff authorized by the CISO or designee.

## **IV. RESPONSIBILITIES:**

The CISO is responsible for the oversight of compliance with legislative, regulatory, and contractual obligations affecting protection of Information Assets, approving investigations involving Information Assets; and providing leadership in the investigation and management of security events. The CISO is also responsible for reviewing changes in regulatory and statutory law that impacts information security and updating organizational security policies to align with required security requirements.

The CIO, or designee, is responsible for ensuring that all internally developed Software applications comply with appropriate federal and state regulations and for ensuring that any HHSC developed program code and documentation include a copyright notice.

The IST, or designee, is responsible for identification of digital sources of information and collection of electronic evidence to be used in court cases surrounding HHSC security events as set forth in ITD 132, Management of Information Security Incidents and Improvements policy.

The HHSC General Counsel, or designee, is responsible for reviewing and communicating changes in applicable laws and regulations affecting information security to relevant organizational areas; for providing guidance regarding monitoring of Users; and for maintaining and updating contracts to reflect changing and required legislative and regulatory wording or provisions for security of information.

Corporate Compliance is responsible for reviewing and communicating the effects of Privacy legislation relevant organizational areas; and for providing guidance to Users on their individual responsibilities and the procedures to follow for safeguarding PHI.

HHSC Corporate and Regional Management are responsible for educating Workforce members to maintain awareness of policies that protect Information Assets, and providing notice of the intent to take corrective action against personnel for breach of security policies.

Users are responsible for crediting applicable parties for use of respective Intellectual Property when used for HHSC business and to respect copyright laws; utilizing Information Assets in a manner that is in compliance with legislative, regulatory, and contractual obligations, and for protection and non-disclosure of PII in compliance with HIPAA Privacy and Security requirements.

#### **V. AUTHORITY**

- NIST SP 800-53 (Rev. 4)4).
- Security Standards for the Protection of Electronic Protected Health Information 45 CFR Part 164 Subpart C.
- 45 CFR 164.308(a)(2).
- 45 CFR 164.308(a)(3)(i); 45 CFR 164.310(b).

#### **VI. RELATED PROCEDURE:**

None.

#### **VII. REFERENCES:**

- CMP 0008A Retention of Records policy.
- CMP 0021A Privacy and Security Council policy.
- ITD 0005A Information Access System policy.
- ITD 0009 Data Classification policy.
- ITD 0051A Information Security policy.
- ITD 0105A Backup policy.
- ITD 0109A Monitoring policy.
- ITD 0113A User Responsibility policy.
- ITD 0132A Management of Information Security Incidents and Improvements policy.