|  |
| --- |
| **TITLE: Mobile Device Policy**  |
| **DEPARTMENT: Information Technology, Human Resources** |
| **Effective Date:** | **Revised Date:** | **Next Review Date:** |
|  |  |  |
| **Prepared by: Donny Friday, Dir. Of Technology** | **Date: 05/31/21** |
| **Administrative Approval:** Chief Executive Officer, Chief Information Officer, and Compliance Officer |
| CEO: Joe LaRue | Date:  |
| CIO: Chip Burns | Date:  |
| CO: Sharon Grambow | Date:  |
| **All other related polices/procedures/protocols:**  |

SEE LAST PAGE FOR REVIEW HISTORY

**Purpose:**

The purpose of this policy is to define the procedures and restrictions for Users who have legitimate business need to access Sun Health owned Information Systems using personally owned computing devices.

**Scope and Applicability**

This policy applies, but is not limited to, any devices not owned by Sun Health that are used by Workforce members to access company information systems including smartphones, tablets, laptops, desktop computers, and any other device capable of storing corporate data and connecting to a network or the internet.

**Policy Statement**

Workforce members may not access any non-public Sun Health owned Information Systems including the internal network, applications, email, documents, etc. using a non-company owned computing device without obtaining prior approval.

**Procedures**

**General**

1. Information Systems may not be accessed from any device that has not been approved or that fails to meet established Sun Health security standards.
2. PHI and other sensitive information may not be stored on any personally-owned device or media.
3. All security measures deemed necessary to protect Sun Health Information Systems must be employed.
4. Various tools and techniques may be utilized to manage and monitor access from personally-owned devices to protect the security of, and to prevent misuse of, Information Systems including but not limited to:
	1. Deleting or remotely wiping data and applications from personally-owned devices due to:
		1. Lost or stolen devices;
		2. Changes in employment status;
		3. Violation of, or changes to, policy and procedures;
		4. Other circumstances that may put Information Systems at risk.
	2. Tracking of connections to Information Systems such as identification of the device and user, dates, times, duration of access, unusual usage patterns, presence of prohibited applications, and other suspicious activity.
	3. Data collected may be used for investigation of possible breaches and/or misuse.
5. Workforce members must employ reasonable physical security measures to protect devices against being lost or stolen, and to prevent unauthorized access to Information Systems.
6. Workforce members shall immediately report to the HIPAA Security Officer any security incidents including:
	1. Virus or other malware on the device;
	2. Lost or stolen devices;
	3. Unauthorized access, disclosure, or loss of company information;
	4. Other security risks to Information Systems.
7. Sun Health is not liable for the loss, theft or damage of any personally-owned devices.
8. Sun Health will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings.

**Smartphones and Tablets**

1. All devices must be protected by a strong password, PIN, biometric, or other approved authentication method.
2. Devices shall automatically lock and require re-authentication after no more than 15 minutes of inactivity.
3. All devices must be encrypted using approved methods.
4. Installation of various applications, including anti-malware, may be required based on the device.
5. Removing restrictions imposed by the device manufacturer to gain access to the operating system to unlock features and install unauthorized software, known as Jailbreaking (iOS) and rooting (Android), is strictly prohibited.
6. Available features designed to locate lost or missing devices must be enabled.
7. Transmitting of PHI or other Sensitive information is approved through authorized, secure means only.
8. Applications must only be installed from approved sources such as Google, Apple, or Microsoft app stores. Installation of apps from un-trusted sources is forbidden. Users may not load pirated software or illegal content onto their devices.
9. Devices must be kept up to date with manufacturer or network provided patches.

**Computers (Laptops and Desktops)**

1. Users must create strong passwords consistent with Sun Health policy.
2. Automatic account locking or logoff must be configured after a period of inactivity consistent with Sun Health policy.
3. Laptops that are transported outside of a private residence, office, or other secured area must be encrypted.
4. Computers must have installed, up-to-date anti-virus and anti-malware software.
5. Users may not install software from untrusted sources and may not load pirated software or illegal content onto their devices.
6. Computers must be configured to automatically download and install manufacturer provided software updates.

**Enforcement & Exception Handling**

Failure to comply with this policy, associated procedures and guidelines may result in disciplinary actions up to and including termination of employment or termination of contracts. Legal actions also may be taken for violations of applicable regulations and laws.

Request for exceptions to this policy must be submitted in writing. Prior to official approval of any exception, this policy must continue to be observed.

**Definitions**

**PHI** -Protected Health Information.

**Information System** -Meansany combination of [information technology](http://en.wikipedia.org/wiki/Information_technology) and people's activities that support operational, management and decision-making processes. A system normally includes hardware, software, information, data, applications, communications, and people.

**Workforce Member** -Means employees and other persons whose conduct, in the performance of their work, is under the direct control of the organization, whether or not they are paid by Sun Health. This includes full and part time employees, contractors, affiliates, associates, students, volunteers, and staff from third party entities who provide services.

**Users** -Are the individuals, groups, or organizations authorized to access information assets.

**Distribution**

This policy should be distributed to applicable Workforce Members. Recipients of this policy must acknowledge their receipt and understanding of this policy by referring any questions or problems with the policy within ten days of the issue date to the HIPAA Security Officer. If no questions or problems are stated, it will be assumed that the policy has been read and understood.

**Applicable Regulations**

|  |  |
| --- | --- |
| **HIPAA Security Rule** | **45 CFR Part 160 and Subparts A and C of Part 164** |
| Workstation Use | §45 CFR 164.310(b) |
| Security Management Process  | §164.308(a)(1), §164.308(a)(1)(ii)(A), §164.308(a)(1)(ii)(B) |
| Contingency Plan  | §164.308(a)(7)(ii)(E) |

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date: | Reviewed/Revised by: | New Changes | No Change√ | Revision(s): State reason for revision  | INITIALS |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

This policy is subject to the Master Service Agreement, confidential, and for internal business use only.

Nothing contained herein shall be construed as conferring by implication, estoppel or otherwise any license or other grant of right to use this customized intellectual property of BOC, except as expressly provided herein. This intellectual property was created for clients of blue orange compliance (BOC) for their sole and exclusive use. This property is not intended for the resale or reuse, except as BOC may voluntarily choose to transfer such property, in full, or in part. All customized work has a lifespan where it remains applicable for a client. BOC is not responsible for misprints, out-of-date information, technical inaccuracies, typographical or other errors appearing in this intellectual property. All information and related materials it contains are provided "AS IS", and is not intended to be legal advice. BOC makes no representation or warranty whatsoever regarding the completeness, accuracy, currency, or adequacy of, or the suitability, functionality, or availability, of the information or materials it contains. By ongoing use of this material without the availability of a current support contract from BOC, client assumes the risk that the information and materials may no longer be complete, accurate, in date, or may not meet your needs and requirements.