Information Technology Acceptable Use Policy

I. Purpose

This policy defines the acceptable use of all TidalHealth ("TIDALHEALTH") computer and communication system assets.

II. Scope

This policy applies to all employees and third-parties with access to TIDALHEALTH electronic information resources. While this Policy generally addresses technology concerns, it does not stand-alone. All use of technology at TIDALHEALTH or in connection with its information systems must also comply with all other TIDALHEALTH policies and procedures.

III. Policy

A. System Usage

1. Only equipment authorized and approved by the Information Services Department ("IS Department") may be used with or connected to the TIDALHEALTH corporate network. The use of this equipment must adhere to the Asset Management and Change Management policies.
2. It is the responsibility of all staff and authorized users of the information systems of Peninsula Regional to adhere to TIDALHEALTH's policies as well as HIPAA requirements for accessing protected health information and promoting the security of the information contained within our information systems. An individual's access to our systems is determined based upon their position, the duties and responsibilities associated with their specific role. Access is granted for that specific purpose and that purpose alone. If an individual has an interest in accessing records that do not pertain to their regular work duties and responsibilities, they are to contact the HIM department for assistance and to initiate the Release of Information process (where authorized). This would include, but not limited to, access to an individual's own medical record, a co-worker's record or that of any family member.
3. Sharing of an individually assigned TIDALHEALTH Device with Other People is prohibited – Individuals must not share their TIDALHEALTH issued device with any other person.
4. Reasonable Personal Use Of Computer And Communications Systems - TIDALHEALTH allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use must be consistent with conventional standards and TIDALHEALTH Code of Ethical Conduct. For example, electronic mail must not be used to distribute or display messages or graphics which may be considered by some to be disruptive or offensive (such as sexual jokes or pornography).
5. Use at your own Risk – End Users access the Internet with TIDALHEALTH facilities at their own risk. TIDALHEALTH is not responsible for material viewed, downloaded,

or received by users through the Internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

6. Activity Monitoring – Users must be aware that their activity while using TIDALHEALTH systems is monitored and recorded. This information may include web sites visited, files downloaded, time spent on the Internet, email received or sent and related information.
7. Unattended Active Sessions – Per the Clean Desk policy, users must not leave any device unattended without logging out or invoking a password-protected screen saver
8. Session Timeout – Per the Access Control policy, all systems are subject to session timeout for no activity of 15 minutes or less at which point the contents of the screen are obscured. If sensitive information resides on any device, the screen must immediately be protected with a password protected screensaver or screen lock, or the machine turned off, whenever a System User leaves the location where the device is in use.

B. User IDs and Passwords

1. Personal User IDs Responsibility - Users must be responsible for all activity performed with their unique user IDs. They must not permit others to perform any activity with their user IDs, and they must not perform any activity with IDs belonging to other users.
2. Access Code Sharing Prohibited - TIDALHEALTH computer accounts, user IDs, network passwords, voice mail box personal identification numbers, credit card numbers, and other access codes must not be used by anyone other than the person to whom they were originally issued.
3. Sharing Passwords - Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Information Services Department staff must never ask users to reveal their passwords.
4. Strong Passwords – Per the Password Management policy, users must choose passwords that are difficult to guess and adhere to complexity requirements. For example, users must not choose a dictionary word, derivatives of user IDs, common character sequences, details of their personal history, a common name, or a word that reflects work activities.
5. Typing Passwords When Others Are Watching – Per the Access Control policy, System Users must never type their passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.
6. Password Proximity To Access Devices – Per the Password Management policy, users must never write down or otherwise record a readable password and store it near the access device to which it pertains.
7. Passwords In Communications Software - Per the Password Management policy, users must not store fixed passwords in dial-up communications programs, Internet browsers, or related data communications software at any time.
8. Suspected Password Disclosure - Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

C. Electronic Messaging

1. Identity Misrepresentation – System users must not misrepresent, obscure, suppress, or replace their own or another person's identity on any TIDALHEALTH electronic communications.
2. Handling Attachments - Only TIDALHEALTH approved email attachments will be accepted from external senders.
3. No Guarantee of Message Privacy - TIDALHEALTH cannot guarantee that electronic communications will be private. End Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. End Users must accordingly be careful about the topics covered in TIDALHEALTH electronic communications, and should not send a message discussing anything that they would not be comfortable reading about on the front page of their local newspaper.
4. Outbound Electronic Mail Protection of Sensitive Information – Per the Transmission Security and Access Control Policies, all sensitive information to include but not limited to Protected Health Information (PHI), Personal Identifiable Information (PII) and Sensitive Financial Information, must be encrypted when transmitted to third parties.
5. Outbound Electronic Mail Footer - A footer prepared by the Legal Department must be automatically appended to all outbound electronic mail originating from TIDALHEALTH computers. This footer must make reference to the possibility that the message may contain confidential information, that it is for the use of the named recipients only, that the message has been logged for archival purposes, that the message may be reviewed by parties at TIDALHEALTH other than those named in the message header, and that the message does not necessarily constitute an official representation of TIDALHEALTH.
6. Responding to Personal Information Requests – TIDALHEALTH system Users must never respond to electronic mail messages that request personal or sensitive company information, even from internal sources. The TIDALHEALTH Information Services Department will never request that you perform security duties, such as changing your password, via electronic mail. Any such requests will be confirmed with separate communication from management.
7. Responding to Offensive Messages – System Users must not respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications but instead report these instances to the Information Services Department.
8. Harassing Or Offensive Materials - TIDALHEALTH computer and communications systems are not intended to be used for, and must not be used for the exercise of a System Users' right to free speech. These systems must not be used as an open forum to discuss TIDALHEALTH organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. System Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.
9. Message Forwarding - TIDALHEALTH Confidential information must not be forwarded to any party outside TIDALHEALTH without the prior approval. Messages sent by outside parties must not be forwarded to other third parties unless the sender clearly intended this and such forwarding is necessary to accomplish a customary business objective. In all other cases, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding.

D. Internet and Web Usage

1. Reasonable personal use of the Internet by Users is permitted, if such use is lawful, in compliance with TIDALHEALTH's policies, and does not interfere with the performance of TIDALHEALTH business
2. Posting Sensitive Information – System Users must not post unencrypted TIDALHEALTH material on any publicly-accessible Internet computer that supports any and all anonymously and publicly-accessible services, unless the posting of these materials has been approved by the director of Public Relations.
3. Disclosing Internal Information – System Users must not publicly disclose internal TIDALHEALTH information by posting to any web site, including blogs, newsgroups, chat groups or social networking sites. Such information includes business prospects, products now in research and development, product performance analyses, product release dates, and internal information systems problems. Responses to specific customer electronic mail messages are exempted from this policy.
4. Offensive Web Sites - TIDALHEALTH is not responsible for the content that System Users may encounter when they use the Internet. When and if Users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. When using TIDALHEALTH computers, System Users who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.
5. Blocking Sites - Blocking Sites and Content Types - The ability to connect with a specific web site does not in itself imply that users of TIDALHEALTH systems are permitted to visit that site. TIDALHEALTH may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. TIDALHEALTH will restrict access to sites based on content or reputation not consistent with organizational and/or ethical standards.
6. Social Networking Sites and Personal Webmail Sites– System Users are prohibited from accessing web sites designed for the sole purpose of posting and sharing personal information (as an example social networking sites or non-TIDALHEALTH webmail). Exceptions require the approval of the Information Security Department and must be for documented business purposes. Employees are also prohibited from discussing specific TIDALHEALTH business within any personal home pages they may have established on these sites outside of TIDALHEALTH business hours.

E. Data Storage

1. Establishing Third-Party Networks – System Users must not establish any third-party information storage network that will handle TIDALHEALTH information (electronic bulletin boards, blogs, cloud storage) without the specific approval of the Information Services Department.

F. Internal Systems

1. Eradicating Computer Malware - Any User who suspects infection by a virus or malicious software must immediately call the Information Services Service Desk, and make no attempt to eradicate the malware themselves without help from Information Services Department.

2. Trusted Software Scanning - System Users must not use any externally-provided software unless the software has been scanned for malicious code and approved by the Information Services Department or a local information security coordinator.
3. Prohibition Against All Forms Of Adult Content - All forms of adult content (pornography or what some would consider to be pornography) are prohibited on TIDALHEALTH computers and networks. This includes content obtained via web sites, email attachments, storage media, and file sharing networks.
4. Unauthorized Software And Data Copies - TIDALHEALTH strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet users or other system users make unauthorized copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by TIDALHEALTH. Likewise, TIDALHEALTH allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.
5. Involvement With Computer Malware - Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any TIDALHEALTH computer or network.
6. External Storage Checking - Externally-supplied CD-ROMs, and other approved removable storage media must not be used unless they have been approved by Information Services and checked for malware.
7. Accepting Security Assistance From Outsiders - Users must not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by the TIDALHEALTH Information Services Department. This means that users must not accept offers of free consulting services, must not download free security software via the Internet, and must not employ free security posture evaluation web pages, unless the specific provider of the assistance has been previously approved.

G. Physical Security

1. Positioning Display Screens – Per the Clean Desk policy, the display screens for all computers used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see System Users enter passwords, encryption keys, and other security-related parameters.
2. Locking Sensitive Information - Per the Clean Desk policy, when not being used by authorized System User, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.
3. Custodians For Equipment - The primary user/department of any TIDALHEALTH Device/Asset is considered a Custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a Custodian must promptly inform the Information Services Department. With the exception of portable machines, TIDALHEALTH Device/Assets

must not be moved or relocated without the knowledge and approval of the Information Services Department. Do not leave TIDALHEALTH owned portable devices unattended in any public space.

4. Use Of Personal Equipment – TIDALHEALTH employees must not connect personal computers, devices or peripherals to the TIDALHEALTH corporate network without prior authorization from the Information Services Department. Employees must not use their own personal computers for conducting TIDALHEALTH business unless these systems have been approved by the Information Services Department. Personal mobile devices (i.e. - "Smartphones") must be used in accordance with our Mobile Device Policy.

H. Telephones, Voice Mail and Faxing

1. Sensitive Information On Voicemail - Employees must not record messages containing sensitive information on answering machines and voice mail systems.
2. The transmission of patient information by fax, must be in compliance with the Faxing Patient Information policy. Patient-specific information should be faxed ONLY when it is urgently needed for patient care or required by a third party payer for ongoing certification of payment to insurance companies or physician offices for insurance purposes

I. Security Incident Reporting

1. Reporting Security Events – Any suspected events that may compromise information security or are known to violate an existing security policy must be immediately reported to the Information Services Department. Examples of these events include:

   - Any unauthorized use of TIDALHEALTH information systems;
   - Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed;
   - All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages;
   - Suspected or actual disclosure of Sensitive TIDALHEALTH information to unauthorized third parties.

IV. Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. TIDALHEALTH reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. TIDALHEALTH does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, TIDALHEALTH reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

V. References

CPL: 4.5 Acceptable Use of Assets
ISO/IEC 27002: 8.1.3 Acceptable Use of Assets
HIPAA: Workstation Use 164.310(b) (R)
PCI-DSS: 12.3 Acceptable Usage
NIST: PL-4 Rules of Behavior

VI. Revision History

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Version	09/01/18	09/01/19	Ray Adkins

TIDALHEALTH

INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

ACKNOWLEDGMENT AND CONSENT FORM

I acknowledge that I have received and read the *TidalHealth Information Technology Acceptable Use Policy* dated September, 2018 (the "Policy"), and I agree that I will read any and all future updates thereto. I understand that every employee, physician, nurse, medical professional, and consultant of TidalHealth ("TIDALHEALTH"), and anyone else having access to TIDALHEALTH's information systems or network is required to comply with the Policy and its updates. I hereby consent to, and agree to be bound by, the terms and conditions of the Policy, and I agree to abide by the Policy and the terms of any and all future updates to the Policy.

If, from time to time, I have a concern, knowledge, or information about a possible violation of the Policy, I agree to promptly report the concern to TIDALHEALTH's Department of Information Systems.

Please Print

Name: _____

Signature: _____

Date: _____

Date of Birth: _____

Job Title: _____

TIDALHEALTH Department, Affiliated Physician's Office or Company Name _____

Badge No.: _____

Please promptly remit this form to is.access@peninsula.org or via fax to 410-543-7179 for inclusion in your computer access files.