Title: User Acceptable Use Agreement

Purpose
The purpose of this agreement is to outline the acceptable use of Kootenai Health computer equipment. An acceptable use agreement is not written to impose restrictions that are contrary to Kootenai Health's established culture of openness, trust and integrity.

Acceptable use supports our information assurance program, and protects our health system and partners from damaging actions. Inappropriate use exposes Kootenai Health to risks that include malicious software attack, the compromise of network systems and services, and legal action.

3rd parties/Affiliates/Employees are accountable for compliance with all Security and HIPAA policies and are required to read and understand them.

Applicability
This agreement applies to employees, medical staff, non-employee providers, business partners, contractors, volunteers, affiliates, and trainees. Third parties with access to Kootenai Health systems or data are also accountable for compliance with this agreement. The use of the term "user" in this policy includes all of the individuals listed above.

Special Instructions
Effective security is a team effort involving the participation and support of every Kootenai Health user who deals with information, information systems, or information technology. It is the responsibility of every user to know these guidelines and to conduct their activities accordingly. This agreement requires that users maintain confidentiality indefinitely, even after the contract, work, employment, or any other aspect of involvement with Kootenai Health has ended.

Changes that affect this agreement
We **require** that users follow our User Acceptable Use Agreement and other security policies and that all users IMMEDIATELY notify Kootenai Health of any changes that affect this agreement. This includes, but is not limited to, employee terminations, any suspected data breaches, and any incident that could lead to the degradation of Kootenai Health's security.

General Use and Ownership
1) Communications or stored data may be subject to monitoring, interception and search, and may be disclosed or used for Kootenai Health interests. Kootenai Health will audit networks and systems on a periodic basis to ensure compliance with this agreement.
2) Users should be aware that the data they create on Kootenai systems remains the property of Kootenai Health. Trade secrets, operational details, and any work product shall remain the exclusive property of Kootenai Health and must not be shared with anyone not previously authorized to receive such information (authorization MUST be in writing by a person duly authorized to provide authorization). Kootenai Health Information Technology staff reserves the right to track or otherwise investigate employee acceptable use.

3) Upon termination, users no longer have any rights to Kootenai Health data, intellectual property, trade secrets, operational processes, property or systems beyond that of a member of the general public. Maintaining access to any Kootenai Health property or data will be construed as theft. Accessing any system in any manner inconsistent with that of the general public will be construed as unauthorized access. Kootenai Health reserves the right to report suspected crimes to the appropriate authorities.
4) Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for managing personal use details not addressed in this agreement. Users should consult their supervisor or manager in the absence of department direction.
5) Personally identifiable information (PII), protected health information (PHI), or Health Insurance Portability and Accountability Act (HIPAA) communications will be encrypted if sent outside of the Kootenai Health network (e.g., email, compact disc, flash memory storage device, etc.). Text messaging of any personally identifiable information shall be done, only with approval from the IT Security Manager or Senior Management and in accordance with the Kootenai Health Security Manual.
6) Users will immediately report all security incidents, including PII, PHI, or HIPAA breaches, to their immediate supervisor or the Privacy Officer. This includes any item that is lost (or cannot be found after a reasonable attempt to locate it) that contains confidential information.
7) Users using workstations shall consider the sensitivity of the information, including PHI that may be accessed, and minimize the possibility of unauthorized access.
8) Users will not access, store, process, display, distribute, transmit, or view material that is abusive, harassing, defamatory, vulgar, pornographic, profane or racist, that promotes hate crimes or is subversive or objectionable by nature, that encourages criminal activity, or violates local, state, federal or international law.
9) Users may use only employer provided software on their company provided computers and electronic devices. Downloading and/or installing any software shall be done with the approval of the IT Department.
10) This agreement applies to social networking that affects patients or employees, regardless of where the networking is performed.
11) Kootenai Health users will maintain physical and technical safeguards, for all workstations that access PHI, to restrict access to authorized users.
12) Personal computers, tablets and phones MUST NOT be connected to the Kootenai Health secure network. For example; plugging your device into any Kootenai Health network (Computer) jack Kh.Secure and KMC_secure. Personal devices are allowed to be connected to the KH_Guest network only.
13) It is NEVER acceptable to access, store, transmit, or in any way interact with Kootenai Health Confidential data from or to any personal device. This does not prohibit users from getting email and connecting to the Kootenai Health Secure Network on a Kootenai Health owned device such as an issued phone or tablet and/or a personal phone that is authorized by your Director or Vice-President to access email. Please note that phones will be allowed to connect to the Kootenai Health secure network only if they have the email client configured and the user/owner acknowledges and agrees with the Corporate Cell Phone/Device Use Policy.

Appropriate physical measures include:

1) Safeguarding information and Information Technology from unauthorized or inadvertent modification, disclosure, destruction or misuse.
2) Securing laptops that contain sensitive information by using cable locks or by locking laptops inside drawers or cabinets.
3) Reporting any known or suspected computer virus or malware behaviors.
4) Ensuring that monitors are positioned away from public view, or installing privacy screen filters or other physical barriers to public viewing.
5) Not connecting any computing device to a KOOTENAI HEALTH workstation or network, except as authorized by the CIO.
6) Appropriately challenging or reporting any person or persons in non-public areas of the hospital attempting to access any Kootenai Health equipment; who appear to be or are known to be unauthorized.

Appropriate technical measures include:

1) Securing workstation displays (screen lock or logout) prior to leaving the immediate area.
2) Enabling a password-protected screen saver with no greater than a 15 minute "timeout" period.
3) Closing all applications and documents before leaving the workstation for periods exceeding two hours.
4) Ensuring passwords conform to Kootenai Password Standards and are never written or otherwise publically displayed.
5) Ensuring all workstation stored data (i.e., "data at rest") is encrypted.
6) Ensuring all mobile device (e.g., USB drive, "thumb drive", CD/DVD, etc.) PHI data is encrypted.
7) All company owned laptop computer hard drives will be encrypted.
8) Ensuring workstations are left powered on but logged off in order to facilitate after hours' updates.
9) If wireless network access is used, ensure access is secure by following the Wireless and Remote Access policy.
12) All publically facing websites and interfaces must have a valid penetration test complete, before any Kootenai Health Confidential data is connected or presented to such interfaces. NOTE: "Confidential" includes any Protected Health Information (PHI) and electronic Protected Health Information (ePHI).

Physical Security and Proprietary Information

1) Users will take all reasonable precautions to prevent unauthorized access to company private information, corporate strategies, competitor sensitive, trade secrets, specifications, patient lists, and research data. Unauthorized access includes accessing any information not required to perform official duties, including but not limited to patient data, and personnel and pay records.
2) Users will keep all access privileges physically secure and will not share individual accounts, accesses or passwords. Authorized users are responsible for the security of their passwords and accounts. The account owner is fully responsible for the use and activity associated with the account.
3) All computers that are connected to the Kootenai Health network, whether user or company owned, will be continually executing virus scanning and anti-spyware software with current signatures files. The owners of these computers will not store confidential data on these computers unless they are appropriately encrypted and all software is up-to-date.
4) Portable devices (personal or otherwise) will be encrypted, if confidential data is stored, processed, or transmitted to or from the device.
5) Non Kootenai Health systems that store, process or transmit Kootenai Health Confidential data shall be approved by the CIO or his/her designee, prior to allowing the data to be stored, processed, or transmitted to or from these devices.
6) Users will virus-check all information before introducing or uploading it to the Kootenai Health network. Additionally, these devices will run personal firewall software, unless the device operating system does not support such.
7) Users should not open emails received from unknown senders and should report these emails to the Kootenai Health Help Desk at helpdesk@kh.org.
8) Users will not store company-based PII or other confidential data or patient data on personal removable computing devices without prior approval from the IT Security Manager or CIO.
9) Users will pick up printed material in a timely manner from shared printers, fax machines, and other open areas of the hospital, and ensure sensitive information printed materials are kept secure.
10) Printed documents containing PII, PHI, and other sensitive information will be retrieved immediately upon printing.
11) Users will not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
12) Users will not export software, technical information, encryption software or technology, in violation of international or regional export control laws.
13) Unattended Equipment- Any device, equipment, or other item that has or could contain confidential data MUST be managed to ensure that confidential data is not compromised. When unattended, every attempt should be made to lock the screen, place the device into a locked room, or ensure that if accessed, cameras would catch the inappropriate review of confidential data. If none of this is possible, the equipment should be turned off, at a minimum.

Passwords

1) Passwords to all systems will be changed at least every 180 days or upon suspicion that a password has been compromised.
2) Passwords will not be shared with others and accounts will not be shared, including with family and other household members when work is performed at home.
3) Users will not provide access to any Kootenai Health system or data to any non-Kootenai Health employee, including family members, without approval by the IT Security Manager or CIO.
4) The Active Directory will automatically disable accounts that have not been accessed in 180 days. If this occurs, the user will need to contact the Help Desk to reactivate their account.
5) Users at Kootenai Health MUST construct the passwords to their accounts (user IDs) that are not easily guessed or predictable. REQUIRED behaviors are:
   a) Construct passwords with a minimum length of 12 characters, and include at least one alphabetic and one numeric character.
   b) Where possible, passphrases 16 characters or longer should be used, as passwords. Passphrases are sentences with proper grammar and punctuation.
   c) Do not construct passwords using dictionary words, names or parts of names, phone numbers, or dates unless used as a passphrase with 16 or more characters.
   d) Do not construct passwords or passphrases using Social Security numbers or any derivatives.
   e) Do not make passwords the same as user ID
   f) Do not make passwords on production systems the same as those used to access systems in non-production environments.

Email

1) Users will not send unsolicited mass-recipient email messages (spam) or other advertising to individuals who did not specifically request such.
2) Users will not use email to harass, through message language, frequency, or size.
3) Users will only use email header information for official purposes and not solicit address information with the intent to harass or to collect replies.
4) Email will not be used to create or forward chain-letter email.
5) The use of email to facilitate private commercial business is not acceptable.

Internet Presence

1) The use of the Internet to facilitate private commercial business is not acceptable.
2) Limited and occasional use of Kootenai Health's systems to engage in personal activities is acceptable as long as it is done in a professional and responsible manner, does not otherwise violate Kootenai Health policies, and is not detrimental to Kootenai Health's best interests.
3) Users will not engage in any blogging that may harm or tarnish the image, reputation or goodwill of Kootenai Health, or any of its employees. Users are prohibited from making any discriminatory, disparaging, defamatory or harassing comments.
4) Users may not attribute personal statements, opinions, or beliefs to Kootenai when blogging. If a user is expressing his or her beliefs and/or opinions in blog, he/she may not, expressly or implicitly, represent themselves as an employee or representative of Kootenai. Users assume any and all risk associated with blogging.
5) Kootenai Health's trademarks, logos and any other Kootenai Health intellectual property may not be used in connection with any blogging activity, except as approved by executive management.
6) Users will not post to newsgroups with their Kootenai Health email address, unless such posting is in the course of business duties.

Unacceptable Use

The following activities provide a framework for activities which fall into the category of unacceptable use and are, in general, prohibited. Users may be exempted from these restrictions while performing legitimate job responsibilities.

1) The storage, installation or distribution of unauthorized software or products not appropriately licensed for use by Kootenai Health (this cannot be exempted if it violates any law or copyright requirement).
2) Introducing, coding, compiling, storing, transmitting or transferring malicious software code, including but not limited to viruses, worms and Trojan horses.
3) Uploading or downloading executable software (e.g., screensavers, entertainment software, games, etc.) without prior approval from the IT Security Manager or CIO.
4) Gambling, wagering or placing any online bets.
5) Using a Kootenai Health computing asset to procure or transmit material that is in violation of sexual harassment or hostile workplace laws.
6) Making fraudulent offers of products, items, or services originating from any Kootenai Health account.
7) Making warranty statements, expressly or implied, unless it is a part of normal job duties.
8) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.
9) Relocating or changing equipment, or the network connectivity of the equipment, without prior authorization from the Kootenai Change Control Review Board, IT Security Manager or CIO.
10) Network port scanning or security scanning without prior approval of the IT Security Manager or CIO.
11) Executing any form of network monitoring which will intercept data not intended for the employee's computer, without prior approval of the IT Security Manager or CIO.
12) Circumventing user authentication or security of any host, network or account.
13) Interfering with or denying service to any authorized Kootenai Health employee in support of their official duties.
14) Using any program, script, command, or sending messages of any kind, with the intent to interfere with or disable another employee’s session or account.
15) Providing information about or lists of Kootenai Health employees to parties outside Kootenai Health, except in support of their official duties.

Mobile Devices

Mobile device security (laptops, phones, tablets, etc.)

1) Users should never loan a mobile device to any other person
2) Mobile devices left in vehicles should be avoided. If unavoidable, mobile devices should be locked in trunks or other locking compartments. If the device cannot be locked in a trunk or other locking compartment, the device should be hidden from view and the vehicle should be locked.
3) Password/passphrases should NEVER be stored with a portable device.
4) All mobile devices MUST have a password set.
5) All Mobile devices with Kootenai confidential data including email, patient data, and any other data that should not be published on a publically facing system must be encrypted.
6) Mobile devices are required to have antivirus software installed and updated if they have any access to Kootenai confidential data including email, patient data, and any other data that should not be published on a publically facing system.
7) Prior to purchase of a mobile device, review Kootenai Health policies and information specifically related to mobile devices. See Corporate Cell Phone/Device Use policy.
8) Avoid using unencrypted usernames and passwords when accessing networks, applications, or files.
9) Avoid storing sensitive or confidential information on the device whenever possible, and encrypt the information when it must be stored on the device.
10) When carrying Mobile devices on an airplane, do not check the luggage; ensure that you carry it on with you and keep it with you.
11) Enable Only Required Applications or Services
    a) Restrict the “apps,” services, etc., on the device only to those needed. Disable or remove all others. This action will reduce the exposure of the device to viruses and malware. It may also enhance the performance of the device and may extend battery life.

b) Review security settings on required applications, and set to be as strict as practical.

12) Report Lost or Stolen Devices
    a) Helpdesk can be contacted at helpdesk@kh.org or at 208-625-5555.
    b) Report lost or stolen devices immediately.
    c) Helpdesk will remotely wipe the device, deleting all data on the device.
13) Back-up Device
    a) In the event that sensitive or confidential information must be stored on the device, back up the device regularly. This is important if the device is lost, stolen, or damaged.
14) Keep Power to the Device
    a) There is risk when a mobile device loses power that information could be lost, so it is important to keep the battery charged.
15) Dispose of the Device Properly
    a) Make certain all sensitive or confidential information is removed from the device when it is no longer going to be used (i.e., is replaced by a more modern device).

16) Data traveling over public networks (coffee shops, colleges, motels, and other places that allow customers to connect to the network) should be considered unprotected. If you need to send any Kootenai Confidential data over such networks, you MUST connect to Kootenai Health through VPN or an IT approved secure connection methodology.

Under no circumstances is a user of Kootenai Health authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Kootenai Health owned resources.

This agreement, regarding access to confidential data entrusted to Kootenai Health, is made between Kootenai Health District, dba Kootenai Health ("Kootenai Health") and _____.

Agreed this date: _____

By (Signature): _____

Printed Name and Title: _____

Company Name: _____

Address: _____

Telephone/Fax: _____