



Name: _____

School/Program: _____

Instructor: _____

Date: _____

STUDENT PACKET: To Complete

Thank you for your interest in Kootenai Health as a clinical site. In this packet you will find several important forms to review, sign, and submit to Kootenai for your student record. They include:

- Statement of Understanding
- Student Role Description
- Security Agreement
- Ethical Standards Form
- Confidentiality Agreement
- Emergency Code Orientation
- HIPAA Orientation
- Patient Rights
- Cleanliness and Quietness Bundle

Print out this packet and complete the forms.

You will be fully eligible to complete a Kootenai student experience by:

- 1) Reading through the Student Packet: For Your Information
- 2) Completing this packet
- 3) Registering with CPNW and completing the Clinical Passport and Modules at cpnw.org
- 4) Receiving a Kootenai student badge

If you have any questions about the material in this packet contact Student Services at 208-625-6078 or studentservices@kh.org.

Thank you,

Student Services

01/2019



STATEMENT OF UNDERSTANDING

My signature indicates that I reviewed and understand the policies and procedures given to me in the Student Packet: For Your Information, which include the following:

- Professional Appearance Policy
- Hospital Access Control Badges
- Confidentiality Agreement
- Kootenai Health Main Campus Parking Policy
- Infection Prevention Education
- Smoke Free & Tobacco Free Environment
- Patient Bill of Rights and Responsibility
- Event Notification Report
- Safety Orientation
- Notice of Non Discrimination
- Language Translation
- Restraint and Seclusion
- Clinical Communication ISBARD

I also have reviewed the forms and agreements in the Student Packet: To Complete, and I agree to comply with all its terms and conditions.

Signature

Date



Kootenai Health Student Role Description

Role Title: Student

Department: As Assigned

Reports To: Student Services

Role Description:

Students will apply their knowledge and skills under the guidance of a program instructor and/or Kootenai Health designated preceptor. The Kootenai Health employee will be present at all times to provide guidance and assistance to the student to gain knowledge, skills and judgement necessary to perform competently in their educational program.

Student Minimum Qualifications:

The program will select and adequately prepare students for participation in the education experience at Kootenai Health. Eligible students must be in good standing within their program and remain compliant with the following items:

- Respects the safety and well-being of the clients in the learning experience
- Recognizes her/his knowledge, skills and abilities, limits of responsibilities, legislative authority and supervision requirements
- Becomes familiar with and follows all Kootenai Health policies, procedures and principles, including those concerning confidentiality of patient health care information (HIPAA).

Training Requirements:

- Student Orientation Training
- Ongoing orientation and education with designated Kootenai preceptor
- Medical Record training (if applicable to learning experience)
- Additional education may be required based on the assigned learning environment

Physical Requirements:

- Frequent reaching, stooping, bending and twisting.
- Able to use fine motor skills. Able to record activities, document interventions (if applicable)
- Ability to lift up to 25 pounds
- Communication with patients, physicians, families and Kootenai staff in person.
- Work with equipment and manipulate equipment settings as supervised by Kootenai staff.

Work Environment:

- Kootenai Health operates 24 hours per day each day of the year. The student will comply with the learning experience schedule as identified by the educational program and Kootenai Health. Regular and predictable attendance is required
- Education experience may be performed in a variety of locations inside/outside of Kootenai Health, such as outpatient Kootenai Clinics and offices.
- The educational experience is normally performed in a typical interior work environment
- Work environment involves exposure to potentially dangerous materials and situations that require following extensive safety precautions and may include the use of protective equipment.
- Potential exposure to hostile individuals

Role Duties:

- The academic program shall design and deliver in advance, the desired content, objectives, and outcomes associated with the experience, along with any documentation that would objectively validate the experience with regard to identified learning objectives.

Hospital Values:

- Student behavior will reflect the values of Kootenai Health at all times. Students will uphold Kootenai Health rules, policies, procedures, and standards of professional conduct.

Acknowledgement:

I, _____, acknowledge review of this role description and can perform the essential functions of the student role with or without accommodation. If accommodation is needed, I will take the responsibility to clearly communicate what I feel is reasonable to the manager of this position



KootenaiHealth 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) Information Technology department personnel will lock accounts not accessed over a 90-day period.

- 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: _____



ETHICAL STANDARDS

To provide patient safety, well-being, and comfort to the greatest possible extent.

- To be honest, fair, respectful, confidential and trustworthy in all of my Kootenai Health activities and relationships.

- To adhere to applicable laws, regulations and policies.

- To Identify and prevent conflicts of interest between work and personal affairs.

- To accept responsibility to improve all services.

- To provide a safe work place and to protect the environment.

- To provide equal and fair opportunity to every member of the Kootenai Health community.

- To provide a personal work environment that is free from verbal, physical and sexual harassment.

- To protect Kootenai Health resources and assets.

- To be responsible for and contribute to a culture where ethical conduct is recognized, valued and exemplified by everyone.

How I can support these standards...

1. Strive to do the right thing for the right reason.
2. Understand and apply the components of Kootenai Health's Standards in my day-to-day work.
3. Always obey the law.
4. Maintain the integrity of my coworkers, physicians, agents, consultants and others by helping them to understand Kootenai Health's ethics.
5. Share information only with those who have a need to know.
6. Refuse bribes, kickbacks, and inappropriate referrals.
7. Seek answers to questions and concerns by talking to a supervisor, department director, Kootenai Health's Compliance Officer, a Human Resource Representative or call the Ethics hotline (1-877-631-0019).
8. Know and follow my rights as an employee to pursue any ethical concerns.

My signature indicates that I have reviewed and understand the ethical standards and I will conduct myself and perform my duties in a manner that supports Kootenai Health's ethical standards.

Signature

Date

Name (Please Print First, Middle Initial, Last)



KOOTENAI HEALTH WORKFORCE

CONFIDENTIALITY AGREEMENT

I _____ understand that Kootenai Health has a legal and ethical responsibility to maintain patient privacy, including obligations to protect the confidentiality of patient information and to safeguard the privacy of patient information.

In addition, I understand that during the course of my employment/assignment/affiliation at Kootenai Health, I may see or hear other Confidential Information such as financial data and operation information that Kootenai Health is obligated to maintain as confidential. As a condition of my employment/assignment/affiliation with Kootenai Health I understand that I must sign and comply with this agreement. By signing this document I understand and agree that:

I will disclose Patient Information and/or Confidential Information only if such disclosure complies with Kootenai Health's policies and is required for the performance of my job. My personal access code(s), user ID(s), access key(s), and password(s) used to access computer systems or other equipment are to be kept confidential at all times. (If applicable)

I will not access or view any information other than what is required to do my job. If I have any question about whether access to certain information is required for me to do my job, I will immediately ask my supervisor or the HIPAA Privacy Officer for clarification. I will not discuss any information pertaining to the practice in an area where unauthorized individuals may hear such information (for example, in hallways, break rooms, on public transportation, at restaurants, and at social events). I understand that it is not acceptable to discuss any patient information in public areas even if specifics such as a patient's name are not used. I will not make inquiries about any practice information for any individual or party who does not have proper authorization to access such information.

I will not make any unauthorized transmissions, copies, disclosures, inquiries, modification, or purging of Patient Information or Confidential Information. Such unauthorized transmission include, but are not limited to removing and/or transferring Patient Information or Confidential Information from Kootenai Health computer system to unauthorized locations (for instance, home). Upon termination of my employment/assignment/affiliation with Kootenai Health I will immediately return all property (e.g. Keys, documents, ID badges, etc.) to Kootenai Health Human Resources Department.

I agree that my obligations under this agreement regarding Patient Information will continue after the termination of my employment/assignment./affiliation with Kootenai Health and /or suspension, restriction, or loss of privileges, in accordance with Kootenai Health's HIPAA policies, as well as potential personal civil and criminal legal penalties.

I understand that any Confidential Information or Patient Information that I access or view at Kootenai Health does not belong to me.

I have read the above agreement and agree to comply with all its terms as a condition of continuing employment.

Signature of employee/physician/student/volunteer

Date

Print Your Name

EMERGENCY CODE ORIENTATION

The purpose of emergency code calls is to communicate an emergency quickly and to mobilize expert assistance. Physicians and staff often work in multiple hospitals, each with their own emergency code designations. It is easy to become confused and use the wrong code in an emergency. This has resulted in harm to patients in several states.

The American Hospital Association has recommended a set of codes for hospitals across the nation to use. Kootenai Health has adopted these uniform codes and for greater clarity will add plain language to many of these code calls.

1. **CODE BLUE** - when Heart or Respirations Stop
2. **CODE RED** – for Fire
3. **CODE ORANGE** – for Hazardous Spill
4. **CODE SILVER** – for Weapon or Hostage situation
5. **INTERNAL TRIAGE** – for internal emergency
 - Bomb or bomb threat
 - Computer network down
 - Major plumbing problems
 - Power or telephone outage
6. **EXTERNAL TRIAGE** – for external disaster
 - Mass casualties
 - Severe weather
 - Massive power outage
 - Nuclear, biological, and chemical accidents
7. **CODE GRAY** – for a combative person
8. **AMBER ALERT** – for infant/child abduction
 - No one is permitted to enter or leave the hospital
 - Detain visitors
9. **CODE WHITE** – for patient elopement (when an adult patient has gone missing)
10. **RAPID RESPONSE TEAM** – when a patient's medical condition is declining and needs emergency medical team at the bedside, prior to heart or respiration stopping.
11. **TRAUMA CODE RED** – for emergencies requiring immediate surgical intervention
12. **CODE CLEAR** – When the codes are clear, the hospital operator will page the "Code Name" and then announce "Clear" to indicate the emergency situation is over. Example: "Code Red, All Clear"










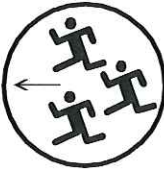
Statement of Understanding

I have read and received the training on Emergency Code Orientation 2015 including a copy of the Security Management Plan, and I agree to comply with all its terms and conditions.

Signature

Date

Emergency Code Calls

| | | |
|---|---|--|
| CODE BLUE  Heart or Respiration Stops | CODE RED  Fire or Fire Drill | CODE ORANGE  Hazardous Spill |
| CODE SILVER  Weapon or Hostage | INTERNAL TRIAGE  Internal Emergency <i>Bomb Threat: Code 77</i> | EXTERNAL TRIAGE  External Disaster |
| CODE GRAY  Combative Person | AMBER ALERT  Infant/Child Abduction | CODE WHITE  Adult Patient is Missing |
| RAPID RESPONSE TEAM  Emergency Medical Team Needed | TRAUMA CODE RED: Level One Trauma CODE CLEAR: Emergency Over CONDITION H: Family Assistance Needed | |

Switchboard Code Line:
625-3333



KootenaiHealth

HIPAA ORIENTATION

As a worker in the healthcare industry, you are affected by the Administrative Simplifications Requirements of HIPAA (Health Insurance Portability Act). You are required by law to follow these rules.

An organization must follow HIPAA if the organization's business activities involve:

- Sending protected health information (PHI) electronically
- Receiving PHI electronically
- If the organization uses any third party vendors who send or receive PHI electronically.

Organizations that must follow HIPAA are called "covered entities".

Protected Health Information (PHI) relates to:

- Person's past, present, or future health
- Healthcare given to the person
- Past, present, or future payment for healthcare given to the person
- And identifies the per or could reasonably be used to identify the person

Business associates are also covered by portions of HIPAA, and must properly safeguard PHI. Examples of business associates are Physicians and Vendors.

In general, penalties for violating HIPAA are criminal and civil penalties.

- Civil monetary penalties include unknowingly, reasonable cause, willful neglect with correction, and willful neglect not corrected and apply to Kootenai Health and its business associates.
- Violating patient privacy under HIPAA has criminal penalties as well which apply to Kootenai Health, our business associates, and any employee who obtains PHI without authorization.

Patients must be notified of any unauthorized activity if their information is improperly accessed, used or disclosed.

The HIPAA security rule establishes national standards for protecting the confidentiality of electronic PHI, the integrity of this information, and the availability of this information. Kootenai Health must ensure the confidentiality, integrity, and availability of electronic PHI, protect against threats to the security of PHI, and protect against any unauthorized use or disclosure of PHI. There are three established security standards:

- Administrative Safeguards-under HIPAA, Kootenai Health must prevent security violations, detect violations, contain violations, and correct violations. Steps for complying with this standard are policies and procedures for:
 1. Risk Analysis-looking at how the organization's electronic PHI might be at risk.
 2. Risk Management-taking steps to address the risks found in the analysis.
 3. Employee Sanction-the organization must punish staff members who do not follow security rules.
 4. Information System Activity Review-looking at records of activity within information systems. For example, the following should be reviewed regularly: Audit logs, Access reports, Security incident tracking records.

Kootenai Health must also have a specific security officer for health information who is in charge of the policies and procedures for keeping PHI safe.

- Physical Safeguards-limit physical access to facilities where electronic PHI is stored making sure only authorized employees have access to these facilities.
 1. All workstations that access electronic PHI should have physical protections, and these protections should ensure that only authorized users have physical access to the workstation
 2. Monitoring the movement of hardware and electronic media with PHI both into and out of the facility, and within the facility.

- Technical Safeguards-only authorized employees should have access to electronic PHI, and Kootenai Health must have ways to record and analyze the activity within information systems that contain electronic PHI.
 1. Kootenai Health must protect electronic PHI from being changed or destroyed improperly
 2. Kootenai Health should have ways of checking that the electronic PHI has not been changed or destroyed without authorization.

The HIPAA Privacy Rule sets the first national standards for protecting the confidentiality of PHI. The goal is to balance two important aspects of healthcare: protecting the privacy of patients, and allowing the flow of health information when needed to ensure high quality healthcare and protect public health. Under HIPAA, Kootenai Health **must** disclose PHI in only two cases:

- When the patient requests access to his or her PHI
- When the Department of Health and Human Services (DHHS or HHS) is doing an investigation

Kootenai Health may use or disclose PHI only when the patient authorizes the use or disclosure in writing or when the use or disclosure is allowed by the Privacy Rule. The Privacy Rule allows disclosure of PHI to the patient, and allows use/disclosure of PHI by Kootenai Health for its own treatment activities, its own payment activities, and its own healthcare operations activities.

Examples are:

1. Treatment Activities
 - Consultation between providers
 - Referral from one provider to another
2. Payment Activities
 - PHI may be used/disclosed by a health plan to obtain premiums, determine responsibility for coverage/benefits, fulfill responsibilities for coverage/benefits, or give or receive payment for healthcare provided to a patient
 - PHI may be used disclosed by a provider to obtain payment for providing care to a patient or to obtain reimbursement for providing care
3. Healthcare Operations Activities
 - PHI may be used/disclosed when Kootenai Health is doing quality assessment and improvement, evaluating provider competency, conducting or arranging for medical services/audits/legal services, performing certain insurance functions, and planning/developing/managing/administering business activities

In all uses/disclosure of PHI Kootenai Health must use/disclose the minimum amount of PHI necessary to achieve the purpose of the use/disclosure.

The Privacy Rule allows use/disclosure of PHI, without the patient's permission, for 12 purposes in the public interest in the following categories:

- Required by law
- Public health activities
- Victims of abuse, neglect, or domestic violence
- Health oversight
- Judicial and administrative proceedings
- Law enforcement
- Decedents
- Organ donation
- Research



2003 Kootenai Health Way
Coeur d'Alene, ID 83814
208.625.4000 tel
kh.org

- Serious threat
- Essential government functions
- Workers' compensation

Kootenai Health must inform patients of their privacy practices and:

- include how the organization may use and disclose PHI
- the organization's duty to protect patient privacy
- how the organization protects and does not protect privacy
- the patient's right to complain about a possible violation of privacy rights, including contact information for making complaints. Kootenai Health provides this for every patient on admission or point of contact.

Patients also have a right to review and obtain a copy of their PHI except psychotherapy notes, information put together for legal proceedings, certain lab results, and certain research information.

Patients have the right to ask to have their PHI amended when PHI is inaccurate or incomplete. If the covered entity agrees to amend PHI, the entity must provide the amendment to anyone who needs it for the wellbeing of the patient.

Statement of Understanding

I have read and received the training on HIPAA for New Employees 2015 including a copy of the Confidentiality and Sanction Policy for HIPAA Violations, and I agree to comply with all its terms and conditions.

Signature

Date



Patient Rights

Patients are provided several rights under the new HIPAA law. These include:

- ❑ **Right to notice of privacy practices – Kootenai Health** has a privacy notice that covers all of the patient's rights. It lets them know how their records are used, and whom Kootenai Health will disclose PHI to. At Kootenai Health, patients are given a copy of the privacy notice in Admitting. Patients then sign that they have received this notice. Notice of Privacy Practice for Kootenai Health is also available on the web.
- ❑ **Right to an accounting of disclosures** – Patients have a right to know when and where their confidential information was released beyond use for treatment, payment and healthcare operations. They can obtain this information from the Medical Records Department.
- ❑ **Right to access** – Patients have the right to access, inspect or get a copy of their health care record. If a patient of Kootenai Health requests a copy of their record, contact Medical Records, Patient Relations or the House Supervisor. The patient will need to sign an authorization for a written copy of their record.
- ❑ **Right to amend** – Patients have a right to request an amendment or change in what was written in their record. This amendment from the patient will then be put in their record with a note of agreement or disagreement from the healthcare provider. Amendments will be done through the Medical Records Department.
- ❑ **Right to request restrictions** – Patients have a right to request that the hospital restrict the release of their confidential information. In other words, they can ask that their hospital stay be kept confidential. This means that we will not tell visitors, clergy, etc. that they are at this facility. Patients that make this request at Kootenai Health will have a "C" next to their name on the computer, and they will not be included in the hospital directory. Patients have the right to request additional restrictions on the use of their PHI for payment and healthcare operations. However, the hospital does not have to agree to the request.
- ❑ **Right to file a complaint** – A patient has the right to file a complaint if they feel that their privacy rights have been violated. Complaints may be directed, the Privacy Officer at Kootenai Health, or to the Secretary of the Department of Health and Human Services.
- ❑ **Right to request alternative communications** – The hospital must accommodate a reasonable request to receive information by alternative means and locations.
- ❑ **Right to request an electronic copy of their records.**



Maintain Confidentiality

There are several things that you can do to maintain a patient's confidentiality. For example:

- ☐ When caring for a patient, share only the information that the caregiver needs to know to provide safe care to the patient. We call this the "need to know" basis.
- ☐ Do not discuss PHI on a phone where the public can overhear the conversation.
- ☐ Avoid discussions about patients in the elevator or cafeteria.
- ☐ Do not leave messages on answering machines regarding the patient's condition.
- ☐ Avoid paging patients or family members over the PA system.
- ☐ Go to a private place and close doors when you need to talk with a patient or their family.
- ☐ Do not post computer passwords on walls, monitors or leave in any easily seen place. Do not share your password with anyone else.
- ☐ Use the "confidential" cover sheet when you fax PHI. If PHI is faxed to the wrong number, tell the facility that received the PHI to shred it or return it, fill out an incident report for tracking purposes and notify Patient Relations for follow-up.
- ☐ Do not send PHI on email unless it is encoded. Our Kootenai Health email is NOT encoded and therefore should not be used to send PHI.
- ☐ Keep your computer screen pointed away from the public.
- ☐ Always exit a program before leave the computer.
- ☐ Keep patient's charts turned upside down at the nursing station or in the bedside chart stand.
- ☐ Be sure to shred or throw any papers with PHI on it in a wastebasket away from public access. Do not take home report sheet notes you have written regarding your patients.
- ☐ Do not post information about patients on social media outlets (face book, MySpace, etc.)

Summary

Protecting a patient's private health information is the job of everyone who works at Kootenai Health. So, be sure to keep yourself informed about HIPAA. All of the confidentiality and HIPAA policies and procedures are on the Intranet under "HIPAA." Contact your supervisor, Patient Relations or the HIPAA privacy officer if you have any questions or are concerned that there has been a HIPAA violation.

My Signature indicates that I have reviewed and understand the Health Information Portability and Accountability Act (HIPPA) and will conduct myself and perform my duties in a manner that supports and upholds these standards.

Name/Date: _____

Signature: _____

Cleanliness and Quietness Bundle
Education and Roll-Out Communication Tool
5/1/2016

Case Statement:

The Kootenai Health Way includes Safety, Compassion, and Engagement as key elements of our cultural work to improve our patient's experience. Recently, a Compassion Steering Committee was formed to guide our efforts to improve our communications, responsiveness and cleanliness/quietness on our patient units. Our HCAHPS data show that we are well below average in these areas. In turn, a sub-committee has developed a bundle of initiatives to help us focus specifically on the following questions:

During this hospital stay, how often was the area around your room quiet at night?

During this hospital stay, how often were your room and bathroom kept clean?

Currently 58.7 percent of patients answer "always" to these questions. This puts us at the 23rd percentile when compared to other hospitals. Our goal is to dramatically improve this score by creating a *noticeably* clean and quiet environment.

Pilot Success:

The Cleanliness and Quietness Bundle has been piloted on 2 South since April 4th, 2016. While it's too early for HCAHPS data results early indicators are promising. There have also been many anecdotal wins such as comments from patients and staff about how noticeably quiet it is on 2-South. The culture has changed and staff are identifying opportunities to reduce the noise further and are reminding visitors and each other of the need to speak softly. The bundle will continue to be monitored and improved and will be rolled out to all units on July 1.

Bundle Elements:

1. **Housekeeping Touchpoints** – Housekeeping will converse with each patient three times a day to make sure we are meeting their cleanliness expectations.
2. **Creation of a Culture of Whisper** – Standards, such as using soft voice tones/whispering, silencing alarms and cell phones, no cart noise, closing patient doors when appropriate, etc., will be monitored and maintained to create a *noticeably* quieter environment (see the Culture of Whisper standards and descriptions).
3. **Key Words at Key Times** – Proactive Rounding and Managerial Rounding will include a reference our efforts to maintain a clean and quiet environment. Staff will also reinforce when washing hands, closing doors, during report, when silencing an alarm, when straightening the patient's room/belongings or at other key moments of service (see the sample key words at key time reference guide).
4. **Engineering Rounds** – Engineering will complete regular rounds to ensure we are correcting chips, dents, scratches, ceiling tiles and other facility repairs.
5. **Quiet Champions** - The unit will appoint a champion each shift to help remind us all if we get a little too noisy.

Your Role:

As you cross onto any patient care unit or area recognize you are entering a clean and quiet zone. Slow your travel, quiet your voice, silence your cell phone, eliminate any cart noise, pick up any trash or clutter and help promote a culture of whisper and a clean environment.

Your Commitment:

I agree to promote a culture of whisper and a clean environment: _____

Signature/Date

Culture of Whisper - Standards

Objective:

To create a culture that creates and sustains a "noticeably quiet" environment on our patient units
To create a culture in which "excessive noise" is an abnormal variation and is not tolerated

| Culture of Whisper Standards | |
|---|--|
| | Description |
| 1. Staff - face to face communication in soft tones or whisper w/in 3-5ft | Close face to face communication is intended to reduce shouting and loud voices across the unit. A diminished, soft tone (even a whisper) can be heard between staff when within 3-5 feet. Social chatter and excessive laughter is kept to a minimum or reserved for break rooms, cafeteria or off-unit areas. Shift change and report may be times to be particularly aware of our voices and communication noise. |
| 2. Patient doors are closed when appropriate | Closed doors will dramatically reduce the noise transmitted into patient rooms. The default should be to close the patient room door unless there are clinical or safety reasons to leave it open. This will be determined by the nurses on the floor. Ancillary and support staff will close the door upon leaving if it was closed upon entering. Also a good time to use "Key Words at Key Times". |
| 3. No cart noise | Transportation carts will be well maintained and repaired to prevent squeaky wheels, rattles, rumbles and other noises. Staff will slow down over bumps, transitions and throughout the unit to minimize cart noise. Any staff transporting excessively noisy carts will be stopped and encouraged to immediately slow down and/or correct their equipment. |
| 4. Alarms silenced quickly (w/in 20 secs) | Equipment, bed, nurse call and other alarms serve a vital purpose and help us respond to safety issues. To reduce the disturbance of these alarms to our patients, they should be acknowledged and silenced as quickly as possible (20 second goal). Our no pass zone efforts are intended to improve our responsiveness and silence alarms as well. Good Key Word at Key Time opportunity. |
| 5. Cell phone/Cisco phone noise minimized and answered within 2 rings | Again our communication tools are vital for our ability to provide safe efficient care. However, loud or unusual ring tones can be very disruptive and create excessive noise. Likewise, unanswered phones become annoying. Cell phones should be set on vibrate or silent mode when ever possible and all phones should be answered within 2 rings. |
| 6. No unannounced construction/cleaning noise | Unfortunately, as we grow and repair our facilities we will have construction noise. We also have floor scrubbers, vacuums and other loud cleaning equipment. Our objective is to provide advanced notice to our staff when excessive construction or cleaning noise is anticipated. Caregivers will then be responsible for notifying their patients. This is a great time to use "key words at key times" and reference our Quiet Kits/earplugs. |
| 7. No slams, bangs, bumps or thumps | There are a variety of other sources of noise. We will all need to prevent slamming doors, gently close cabinets, drawers or hamper lids. Avoid sliding furniture on the floor or into walls. Don't drop heavy objects into the trash containers and gently place items onto counters or surfaces. Please be diligent about identifying other facility noises and other disturbances and reporting them for correction. |
| 8. Dim the lights | Dimmed lighting promotes a quiet environment. The hallway lights should be dimmed during quiet hours (1:00 pm to 3:00 pm) and during the night (8:00 pm to 7:00 am). There are times that there may be exceptions if patient safety is a concern, however the default should be to dim the lights during these hours. |
| 9. Watch your steps | It is important to be conscious of the noise you may make while walking through the unit. Certain shoes are louder than others. Jewelry, keys and other accessories may rattle. Please be aware of heavy footsteps and other noise. |

Definition of "noticeably quiet":

- has the quiet feel and expectations of a library or movie theater environment
- the quietness is contagious and encourages others to talk in a whisper, to silence their phones, and respect our patients desire for peace
- when asked, our patients and visitors will immediately be able to say "my room was always quiet"

Definition of "excessive noise":

- would wake you from a light sleep
- would distract you from normal conversation
- would break your concentration if reading or watching TV

Clean and Quiet - Key Words at Key Times

Objective:

To support our efforts to improve our patients experience around Quietness and Cleanliness
To verbally link our actions to our efforts to improve Quietness and Cleanliness

Roll Out:

Initially we will roll out KW@KT thought managerial and proactive rounding
Subsequent phase will include evaluating for "all staff" roll-out

| Key Time - When you do this: | Key Word - It's a great opportunity to say: |
|--|---|
| Admit a new patient | "We want to make your stay as pleasant as possible. It is important to us that your room is clean and restful . Please let us know if you have any concerns or if we can make you more comfortable." |
| During Shift/Bedside report | "We want to make sure we are coordinating your care between shifts and care givers. Is there anything we can do to make your more comfortable?, is your room clean to your expectations ? Are you able to rest appropriately ?" |
| Wash your hands in front of the patient | "I am washing my hands because cleanliness and infection prevention is really important to us." |
| Shut the patient room door | "I want to close your door to make it as quiet as possible in your room." |
| Silence an equipment alarm | "These alarms are very important for your safety and care, we want to respond quickly to address them and quiet your room as soon as possible." |
| Move or adjust the over-bed table | "Is there anything I can reach for you or straighten up in your room? We want it to be clean and tidy for you." |
| Announce construction, maintenance or cleaning equipment noise | "We really want to make sure it's quiet in here for you. We are going to hear a little construction (maintenance, cleaning noise). The crews tell me it will take about XX minutes. In the mean time, may I close your door, get you a quiet kit or some ear plugs to make you more comfortable?" |
| Other ideas? | |