Information and Technology Policies

Information and Technology Table of Contents

Policy #	Name	Page #
3.00	Information Technology Introduction	3
3.01	Management Information Systems	6
3.02	Electronic Communications	11
3.03	Internet and Internet Services	14
3.04	Internet – Personal Web Sites and Web Logs	17
3.05	Telephone/Instant Message Usage	19
3.06	Employee Responsibilities for Protecting System Integrity	21
3.07	Identification and Authentication	26
3.08	Network Connectivity	28
3.09	Malicious Code	31
3.10	Telecommuting	33
3.11	Transportable Media	37
3.12	Downtime Procedures	40

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.00

Subject: Information Technology Introduction

Department(s) Affected/Distribution: All Departments

Effective Date:

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Katy Trail Community Health hereinafter, referred to as KTCH. It serves as a central policy document with which all employees and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides managers within the KTCH with policies and guidelines concerning the acceptable use of KTCH technology equipment, e-mail, internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all KTCH employees or temporary workers at all locations and by contractors working with the KTCH as subcontractors.

Scope

This policy defines common security requirements for all KTCH personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to volunteers and information resources owned by others, such as contractors of the KTCH, entities in the private sector, in cases where KTCH has a legal, contractual or fiduciary duty to protect said resources while in KTCH custody. In the event of a conflict, the more restrictive measures apply. This policy covers the KTCH network system which is

comprised of various hardware, software, communication equipment and other devices designed to assist the KTCH in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any KTCH domain or VLAN, either hardwired or wireless, and includes all stand-alone equipment that is deployed by the KTCH at its office locations or at remote locales.

Acronyms / Definitions

The following are common terms and acronyms that may be used throughout this document.

CDO – Chief Dental Officer
CEO – The Chief Executive Officer is responsible for the overall privacy and security practices of the company.
CFO - The Chief Financial Officer

COO – Chief Operations Officer
CMO – The Chief Medical Officer.
PO – The Privacy Officer is responsible for HIPAA privacy compliance and confidentiality issues.
DoD – Department of Defense
Encryption – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
ePHI – Electronic Patient Health Information
External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives USB keys, thumb drives, MP3 Players, iPads, iPhones, and tapes.
FAT – File Allocation Table - The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.
Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
FTP – File Transfer Protocol
HIPAA - Health Insurance Portability and Accountability Act
IT - Information Technology
LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
MPLS – Multi-protocol label switching. This is a type of WAN activity.
NTFS – New Technology File Systems – NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.
SOW - Statement of Work - An agreement between two or more parties that detail's the working relationship between the parties and list's a body of work to be completed.

Privileged Users – system administrators and others specifically identified and authorized by KTCH management.
User - Any person authorized to access an information resource.
Users with edit/update capabilities – individuals, who are permitted, based on job assignment, to add, delete, or change records in a database**.**
Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.
Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.
VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.
VPN – Virtual Private Network – Provides a secure passage through the public Internet.
WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.

Each of the policies defined in this document is applicable to the task being performed – not just too specific departments or job titles.

Privacy Officer

The KTCH has established a Privacy Officer (PO) as required by HIPAA. This PO will oversee all ongoing activities related to the development, implementation, and maintenance of the KTCH privacy policies in accordance with applicable federal and state laws. The current PO for the KTCH is:

Morgan Lynch
mlynch@katyhealth.org
P: 660-826-4774 Ext. 811
F: 888-979-8868

The site managers in collaboration with the PO are responsible for presenting security enhancements and features that have been implemented to further protect all sensitive information and assets held by the KTCH. They will complete a quarterly walk through and present the results at the quality staff meetings and to the board quality committee.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.01

Subject: Management Information Systems

Department(s) Affected/Distribution: All Departments

Effective Date: 09/24/15

Origination Approval: Mary Nell Strautman **Date:** 09/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:
BILLING SYSTEM (any systems containing PHI)

KTCH purchased computer software for a data collection and information system. Policies and procedures will be guided by protocols of the vendor's (IMS, Dentrix, ECw, Blackbaud, DRVS) system reference manual.

DATA ENTRY

KTCH's billing system is designed to provide scheduling, billing, patient demographic and personal health information, medical and dental procedures, and diagnosis information that can be used by those responsible for decisions while complying with the multitude of reporting requirements.

1. Patient Service Representative's (PSR) data entry is restricted to entering/updating patient demographic and payer source information, printing bills, and entering payments.
2. Administrative data entry is restricted as follows:
    a. The Billing staff may enter any necessary
    changes to patients' accounts, post charges, payments, and adjustments.
    b. The Billing specialist may enter and/or modify new
    third party carriers, service code charges, zip codes, new provider information, finance codes, program restrictions and other data management maintenance programs at his/her own discretion.

c. The IT Optimization Committee is responsible for any changes to the set-up of the system as deemed necessary. d. The CFO has the final responsibility for the set-up and maintenance of the billing system.

DATA EDITING

DAILY
Each PSR entering information will run daily listing reports each day. The daily listing reports will be edited for accuracy and reconciled to supporting information (deposit slips, schedule log for next day, and daily encounter log which shows all payments for the day).

Electronic billing reports and claims are to be reviewed by designated employees for each insurance type for completeness, reasonableness, and accuracy before transmitting the claims for payment. All batches of claims submitted on paper are to be reviewed by designated employees for each insurance type for completeness, reasonableness, and accuracy before mailing the claims.

The designated employee, when reviewing Explanation of Benefit reports for rejected claims due to a billing error, will make corrections or changes to patients' accounts, third party carrier information and other data as appropriate. The designated employee will review electronic billing reports per batch for accuracy, reasonableness, and completeness.

Any adjustments deemed necessary from the editing process would be made on a daily basis.

Statements are system generated daily.

MONTHLY
End of Month finance reports will be generated on a monthly basis. The End of Month reports will be reviewed by the CFO for reasonableness, completeness, and accuracy.

The Accounts Receivable staff will edit and reconcile the billing system (subsidiary accounts receivable) to the General Ledger accounts receivable monthly. Any adjustments deemed necessary from the editing process will be made on a monthly basis and reviewed and approved through the use of journal entry by the CFO.

ANNUALLY
The accounting staff and CFO will review year-end reports for reasonableness, completeness, and accuracy.

DATA BACKUP
ROUTINE
The servers that are housed at the clinic facility are backed up according to the backup schedules defined in the IT agreement (JMark). Please reference Schedule D in the IT agreement for the specific components of routine backup. ..\..\..\..\Grants & Contracts\Contracts\JMARK.

SYSTEM SECURITY

PASSWORDS
A password is necessary for anyone to log in to any of the vendor systems. Each user will be assigned a temporary password and is responsible to keep their password confidential.

RESTRICTIONS
Staff are restricted based on job title. The IT Optimization Committee will review at least annually.

CONFIDENTIALITY
All patient information is confidential, and every effort should be made to ensure access to the patient's information/medical record is limited to authorized personnel. Personnel who are authorized to access patient information/medical records, within the scope of their duties, which include all staff.

Every employee, Business Associate, student, job shadower, and volunteer of KTCH is required to sign a statement of confidentiality Health Insurance Portability and Accountability Act (HIPAA) applies to all employees.

Computer screens, printers, and faxes are to be kept from the access and view of patients whenever possible.
PHI may not be released externally without a written request by the patient, except as required by law and/or the KTCH privacy statement. Medical records staff handles all such requests.

PHYSICAL PROTECTION

ENVIRONMENT
The computer system and all its apparatus will be properly wired and set-up as designated by the vendor and kept in a dry temperature controlled server area. The equipment will be kept locked, and only a limited number of authorized staff will have access to the controlled area. The equipment may not be moved without authorization of the CEO, CFO, COO. Proper insurance will be maintained on all equipment.

HARDWARE
The CFO is responsible for retaining, on an as needed basis, necessary repairs to hardware to ensure minimal interruptions in operations due to hardware problems.

SYSTEM SECURITY & MAINTENANCE
Vulnerability Scanning
Vulnerability assessments of computers connected to the network are performed in real time. If vulnerabilities are identified, appropriate security measures will be taken to mitigate, and correct issues identified. Corrective actions will also be taken, if necessary, to harden computers and network against future threats and/or vulnerabilities.

Host Intrusion Detection
Intrusion detection is monitored at the firewall level on an on-going basis. The IT support team will troubleshoot and identify IP addresses that are connected to suspicious activity and determined if it is harmful to the environment. If an intrusion is determined to be harmful, IT support team will take measures to block the IP range of the intrusion and block additional traffic associated with the IP range.

Patch Management
Patch management of computer systems will be conducted on a monthly basis in order to fix security vulnerabilities. Trained IT support team will maintain a current knowledge of available patches and decide what patches are appropriate for each computer system. IT support team will test systems after installing patches to ensure that patches are properly installed. IT support team will document patches installed and any changes in configuration of systems.

IT Support
When IT issues are encountered, IT support team member is contacted for support. IT support team will troubleshoot problems and provide guidance to KTCH employees on corrective actions that need to be taken to correct reported issues. IT support team will generate a ticket in the ticketing system that documents the time taken for resolution and the steps implemented to correct issues reported.

Violations of System Security and maintenance will be reported to the PO. Violations can result in disciplinary action and/or termination.

PASSWORDS
A user specific password is necessary for anyone to log in to any vendor system. All user specific passwords will be kept confidential.

PHYSICAL PROTECTION

HARDWARE
Maintenance and repairs of the computer will be done only by a trained IT support team that has experience as a hardware technician.

SOFTWARE
Software support from the vendor will be sought in resolving problems or updates that arise.

PERSONAL AND LAPTOP COMPUTERS

PHYSICAL PROTECTION
Computers and computer apparatus will be properly wired and set-up as designated by the vendor and kept in a dry temperature controlled server area. The equipment will be kept under lock and key during hours of closed operation. The equipment may not be

moved without authorization of the CEO, COO, CFO. All capital equipment will be listed and maintained as per the fixed asset policy. All minor equipment will be tagged and added to the inventory list. A trained computer technician will make any necessary repairs.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.02

Subject: Electronic Communications

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:

Electronic mail (e-mail) and other internal computer files provided by KTCH are to be used for business purposes only and should be treated professionally, with the same care and formality as any written, non-electronic correspondence or any other business communication. Use of KTCH computer equipment for personal reasons is unacceptable, and KTCH will take steps to prevent prohibited uses of e-mail communications and other internal computer files.
Inappropriate and, therefore, prohibited e-mail and other electronic media communications and uses include, but are not limited to the following:

- Personal messages or emotional responses to business memoranda of an emotional nature, gossip, personal information about yourself or someone else. Avoid any impetuous negative responses to something you have read or heard.
- Messages that, in any way, may be disruptive, offensive to others, or harmful to morale, including, but not limited to: sexually explicit images, messages or cartoons; ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of other based upon their race, national origin, sex, sexual orientation, age, disability, or religious or political beliefs.
- Messages concerning non-KTCH commercial ventures, religious or political causes, outside organization or other non-job-related activities.
- Messages that encourage or disseminate chain letters.
- Disseminating or printing copyrighted materials (including articles and software) in violation of copyright laws.

• Any “computer hacking,” including, but not limited to, creating bulletin boards, web pages, or other types of activities not specifically authorized by KTCH.
• Use of any electronic media device to transmit sensitive company documents or data.

In accordance with the 1986 Electronic Communications Privacy Act, KTCH reserves the legal right to access e-mail files and supply law enforcement officials with e-mail and other electronic files. KTCH also reserves the right to enter, search, and monitor the computer files and e-mail of any employee, without advance notice, for business purposes, including but not limited to investigating theft, disclosure of confidential business or proprietary information, unlawful harassment, or monitoring work flow and productivity.

Any time information is transmitted through electronic media there is the possibility that it could be intercepted. Therefore, no confidential information or Protected Health Information (PHI) that includes 1) Medical treatment and other health care information, 2) Billing and payment information, 3) Mental Health Information, 4) AIDS or HIV information, 5) Other as determined by Patient, may be transmitted unless in accordance with established encrypting protocol . If an employee is uncertain whether information is confidential, err on the side of caution and obtain approval from the Privacy Officer (PO) before transmitting it.

KTCH faxes, copiers, and mail systems; including e-mail, or other electronic communications that are composed on, sent from, or received by computer hardware and/or software owned by KTCH is the property of KTCH. Personal business should not be conducted through these systems. KTCH reserves the right to monitor, read, and publish any such communications wherever there is a business need to do so. Employees using this equipment for non-business-related purposes have no expectation of privacy, and may be subject to discipline up to, and including, termination for inappropriate non-business-related use of such equipment.

Employees of KTCH should not attempt to gain access to other employees’ files, email, or other electronic communications without the latter’s expressed permission. However, leadership and management reserve the right to monitor or read any employee’s e-mail or other electronic communications, or to enter any employee’s e-mail or other electronic media files wherever there is a business need to do so.

KTCH obtains the written acknowledgement/agreement of its employees to the monitoring of these e-mails and other electronic communications, normally at the time of hire. Employees who were on staff at the time that this policy was created have been informed of this policy and have given their written consents to adhere to the policy.
Deleted or other electronic communication can be retrieved from any KTCH computer network. Therefore, employees of KTCH should avoid inappropriate and prohibited e-mail and other electronic communications altogether.

KTCH management has the right to monitor telephone conversations and voice mail messages at any time. Inappropriate conversations or voice mail messages could result in disciplinary action up to and including termination.

Generally, while it is **not** the practice of KTCH to monitor the content of any electronic communication, KTCH is responsible for servicing and protecting KTCH's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

KTCH reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as KTCH policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others by posting the "KTCH Privacy Statement" on the bottom of all email communication.

Violation of this policy will subject employee(s) to disciplinary action up to and including termination.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.03

Subject: Internet & Internet Services

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:

Any information that KTCH posts on a commercial on-line system or on the internet may be downloaded, duplicated, and used without KTCH's knowledge or approval. No employee should post anything on a commercial on-line system or on the internet without the approval of the CEO. Employees have no expectation of privacy regarding any information stored on or sent to a KTCH-owned computer.

Software piracy is the unauthorized copying, transmitting, downloading, installing, operating, or other use of computer software, in violation of applicable license agreement and/or copyright and other laws. Any unauthorized operation or use of software licensed to KTCH is prohibited. Any unauthorized copying, transmitting, downloading, or installing, or computer software licensed to KTCH is prohibited. Any unauthorized copying, transmitting, downloading, installing, operating, or other use of any other computer software with computer hardware belonging to KTCH or at a facility belonging to KTCH is prohibited.

Internet use is provided to help employee(s) find information that may be useful in the employee's work. While searches are part of the process of finding useful information, an employee may not use internet access provided by KTCH to seek information that is unrelated to the employee's work at KTCH. KTCH will monitor internet use and take disciplinary action if an employee uses internet access for non-business-related purposes during business hours.

KTCH deems all pornographic material inappropriate. Any employee using KTCH internet connection to search for, download, view, or transmit pornographic material will be subject to discipline, up to, and including, termination of employment.

When an employee uses KTCH internet access, that employee is representing KTCH, therefore, that employee should use the same good judgment in all internet transmissions that the employee would use in written correspondence.

GENERAL ACCESS AND ACKNOWLEDGEMENT

It is hereby acknowledged and understood that KTCH owns and controls all hardware, software and files on all KTCH workstations and Network servers, including those files and/or programs created by employees, contractors and consultants.

All employees with a consistent workstation shall be provided with internal or internet e-mail. Employees are required to change network passwords regularly, or at which time it is requested by the network server.

The following are expressly forbidden, and violators are subject to disciplinary action, and may include termination and restitution for loss, damage, or liability accruing to KTCH as a result of these actions:

- Use of the internet to compromise or circumvent the security of another system or computer (including password cracking or attempts to exploit security weakness).
- Use of the Internet to make available credit card numbers, telephone access codes, cellular phone IDs, etc., by persons other than their owner.
- Use of the internet to harass or intimidate other persons whether or not such persons are employed by KTCH.
- Use of the internet to violate or conspire to violate local, state, or federal laws.
- Use of the internet to spread viruses, Trojan Horses, Trojan mules, or other programs intended to circumvent security or cause unauthorized events or damage to occur on another computer.
- Use of the internet to infringe copyrights or patent rights, to include software piracy and redistribution and retransmission of a copyrighted work in its entirety, or in entirety, or in excerpts beyond the bounds of fair use.
- Use of the internet to export data or material restricted by U.S. law (e.g. International Traffic in Arms Regulation (ITA) or Controlled Commodities List (CCL) Items).
- Use of the internet to transmit unsolicited material to a mass audience.
- Use of the internet for unauthorized release of proprietary or material nonpublic information, or confidential patient-specific data (Protected Health Information (PHI) includes 1) Medical treatment and other health care information, 2) Billing and payment information, 3) Mental Health information 4) AIDS or HIV information, 5) Other personal information and what the patient deems confidential.
- Use of corporate facilities to access the internet or intranet for personal financial gain.

• Use of the internet for viewing, transmitting or receiving pornographic material.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.04

Subject: Internet – Personal Web Sites & Web Logs

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:

Personal Web sites, Web logs (blogs) and social media accounts have become prevalent methods of self-expression in our culture. KTCH respects the right of employees to use these mediums during their personal time outside scheduled working hours. If an employee chooses to identify himself or herself as a KTCH employee on a Web site,Web log or social media account he/she must adhere to the following guidelines:

- Make it clear to the readers that the views expressed are the employee's alone and that they do not necessarily reflect the views of KTCH
- Do not disclose any information that is confidential or proprietary to KTCH or to any third party that has disclosed information to the company. Consult the company's social media policy, confidentiality policy and Internet policy for guidance on what constitutes confidential information and appropriate uses of the company internet. Violation of such policies will result in immediate termination of employment.
- Uphold KTCH's value of respect for the individual and avoid making defamatory statements about KTCH employees, patients, partners, affiliates, and others, including competitors.
- Blogging should not interfere with the employee's job or client commitments.

If blogging activity is seen as compromising the center, KTCH may request a cessation of such commentary and the employee may be subject to counseling and, potentially, disciplinary action. For any questions about these guidelines or any matter related to

personal web sites, social media accounts or blogs, contact the manager of Human Resources.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.05

Subject: Telephone/Instant Message Usage

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:
Katy Trail Community Health (KTCH) has established guidelines regarding appropriate workplace telephone and instant message usage.

PROCEDURES:
When using a telephone for business purposes, employees should remember that they represent KTCH and they are creating an impression of not only themselves, but also of KTCH. Employees are to answer calls promptly, in a pleasant, courteous and business-like manner. Employees should say the following, "Katy Trail Community Health, this is (First Name), How may I help you?" Calls must be transferred tactfully, and employees should give accurate and careful answers to caller's questions. Good telephone etiquette is essential at all times.

Telephones located in business/work areas are intended to be used for business purposes and should only be used for personal calls of an abbreviated or urgent nature. Employees should limit making and/or receiving personal telephone calls. An employee who makes and/or receives excessive personal telephone calls during the employee's work hours will be subject to disciplinary action up to and including termination.

Long distance calls made and/or received by employees must not be charged to KTCH with the exception of business calls and personal calls of an urgent or emergency nature. An employee who makes and/or receives personal long distance calls during the employee's working hours or who makes and/or receives long distance personal telephone calls that are charged to KTCH will be required to reimburse KTCH the costs of the calls and may be subject to disciplinary action.

Instant Messaging
Instant messaging is available through the telephone system and is intended to be used for business purposes only. Instant messaging can be monitored by leadership and/or management at any time. Inappropriate use of this system can result in disciplinary action up to and including termination.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.06

Subject: Employee Responsibilities for Protecting System Integrity

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 09/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:
The first line of defense in data security is the individual KTCH user. KTCH users are responsible for the security of all data which may come to them in any format. KTCH is responsible for maintaining ongoing training programs to inform all users of these requirements.

PROCEDURE:

Challenge Unrecognized Personnel - It is the responsibility of all KTCH personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted KTCH office location, you should challenge them as to their right to be there and escort them to the appropriate place. All visitors to KTCH offices must sign in at the front desk or administrative assistant's desk. In addition, all visitors, excluding patients, must wear a visitor identification badge. All other personnel must be employees of the KTCH. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Most KTCH computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. To avoid theft and confidentiality, never leave laptops unattended in public access areas.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly privacy training. KTCH policy states that all computers will have the automatic screen lock

function set to automatically activate upon 5 minutes of inactivity for all staff. Employees are not allowed to take any action which would override this setting.

Home Use of KTCH Corporate Assets - Only computer hardware and software owned by and installed by KTCH is permitted to be connected to or installed on KTCH equipment unless approved by the CEO. Only software that has been approved for corporate use by KTCH may be installed on KTCH equipment. Computers supplied by KTCH are to be used solely for business purposes. All employees must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by KTCH for home use.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the KTCH are the property of KTCH unless covered by a contractual agreement. Software owned by a KTCH employee may be installed on a KTCH device only with the permission of the CEO. Nothing contained herein applies to software purchased by KTCH employees at their own expense.

Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

- Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
- Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
  Exception: Authorized information system support personnel, or others authorized by the KTCH Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

Reporting Software Malfunctions

Users should inform the appropriate KTCH personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the KTCH computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Shut down your computer immediately

- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus!

Report Security Incidents

It is the responsibility of each KTCH employee(s), visitor(s), or contractor(s) to report perceived security incidents on a continuous basis to the appropriate supervisor or security personnel. A user is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the CEO, COO, and/or PO. Users should report any perceived security incident to their immediate supervisor, their department head, or to the CEO, COO, and/or PO.

Reports of security incidents shall be escalated as quickly as possible to the CEO and/or COO. Each member of KTCH must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged, and the remedial action indicated. It is the responsibility of the COO and PO to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the KTCH CEO or COO shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the KTCH and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of KTCH policy and will result in personnel action and may result in legal action.

Users are to immediately report any perceived HIPAA violations to their immediate supervisor, their department head, or to the PO.

Transferring Software and Files between Home and Work

Personal software shall not be used on KTCH computers or networks. If a need for specific software exists, submit a written request to the COO and/or PO. Users shall not use KTCH purchased software on home or on non-KTCH computers or equipment.

KTCH proprietary data, including but not limited to PHI, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the KTCH without written consent of the respective supervisor or department head. It is crucial for KTCH to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer KTCH data to a non-KTCH Computer System, the supervisor or department head should notify the COO and/or PO of the intentions and the justification for such a transfer of data. All data sent outside of the KTCH network should be encrypted if it contains PHI or other sensitive information.

The KTCH Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since KTCH does not control non-KTCH personal computers, KTCH cannot be sure of the methods that may or may not be in place to protect KTCH sensitive information, hence the need for this restriction.

Internet Considerations
Special precautions are required to block Internet (public) access to KTCH information resources not intended for public access, and to protect confidential KTCH information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval is required from the COO before:

- An internet, or other external network connection, is established;
- KTCH information (including notices, memoranda, documentation and software) is made available on any internet-accessible computer (e.g. web or ftp server) or device;
- Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact the COO .
- Use shall be consistent with the goals of the KTCH. The network can be used to market services related to the KTCH, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data–including but not limited to credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services-shall be encrypted before being transmitted through the internet.

De-identification / Re-identification of Personal Health Information (PHI)
As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged unless it is encrypted or secured

De-identification is defined as the removal of any information that may be used to identify an individual of or relatives, employers, or household members.

PHI includes but is not limited to:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.07

Subject: Identification & Authentication

Department(s) Affected/Distribution: All Departments

Effective Date: 09/24/15

Origination Approval: Mary Nell Strautman **Date:** 09/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:
Individual users should have unique login IDs and passwords.

PROCEDURE:
User Login IDs
An access control system shall identify each user and prevent unauthorized users from entering / using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use/misuse of their individual login ID.

All user login IDs are audited at least twice yearly, and all inactive login ids are revoked. The KTCH manager and/or HR department notifies the Health Informatics Specialist and IT vendor upon the arrival and/or departure of all employees and contractors, at which time login ID's are created and/or revoked.

The logon ID is locked/revoked after a minimum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Passwords

User Account Passwords
User IDs and passwords are required in order to gain access to all KTCH networks and workstations. All passwords are restricted by a corporate wide password policy to be of a "Strong" nature. This means that all passwords must conform to

restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of 8 characters long.
Content Requirements - Passwords must contain three of the following; upper case alphabetic characters, lower case alphabetic characters, numeric characters, ~~and~~ or special characters.
Change Frequency – Passwords must be changed no less than every 90 days. Compromised passwords shall be changed immediately.
Reuse - The previous 4 passwords should not be reused.
Restrictions on Sharing Passwords - Passwords shall not be shared, or written down on paper, or stored within a file or database on a workstation and must be kept confidential.
Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens and are never printed or included in reports or logs.

All Documents sent with PHI must be password protected. Password to access the PHI must be sent separate from the PHI documents requested.

Confidentiality Agreement
Users of KTCH information resources shall sign, as a condition for employment, an appropriate confidentiality agreement).

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing KTCH information resources. All vendors will complete a Business Associate Agreement form and it will be maintained with the contract file.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending, or employees are leaving an organization.

Access Control
Information resources are protected by the use of access control systems. Access control systems include both internal (passwords, encryption, access control lists, constrained user interfaces) and external (port protection devices, firewalls, host-based authentication).

Identification and Authentication Requirements
The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.08

Subject: Network Connectivity

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY: Access to KTCH information resources through remote connections devices/software if available, shall be subject to authorization and authentication by an access control system.

PROCEDURE:
Remote Connections

Systems that allow public access to host computers warrant additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness. IT vendor will be responsible for working with electronic health record vendors to obtain reports to provide to the COO concerning any negative impact of the patient portals on the overall network.

Remote access privileges are granted as needed according to the telecommuting policy.

KTCH provides a link to an Internet Service Provider**.** If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the CEO. The appropriate personnel will ensure adequate security measures are in place.

Telecommunication Equipment
Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the CEO and CFO or designee. Telecommunication equipment and services may include but are not limited to the following:

- phone lines

- fax lines
- calling cards
- phone head sets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- call routing software
- call reporting software
- phone system administration equipment
- T1/Network lines
- long distance lines
- 800 lines
- local phone lines
- PRI circuits
- telephone equipment

Permanent Connections

The security of KTCH systems can be jeopardized from third party locations if KTCH's security and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of KTCH systems. The CEO and, CFO should be involved in the process, design and approval.

Emphasis on Security in Third Party Contracts

Access to KTCH computer systems or corporate networks should not be granted until a review of the following concerns has been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

- Applicable sections of the KTCH Information Security Policy have been reviewed and considered.
- Policies and standards established in the KTCH information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to KTCH computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized

users.

- Dates and times when the service is to be available should be agreed upon in advance.
- Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
- A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Firewalls

Authority from the CEO, CFO must be received before any employee or contractor is granted access to a KTCH router or firewall.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.09

Subject: Malicious Code

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY: Katy Trail Community Health (KTCH) is committed to protecting all KTCH computers and servers from malicious coding.

Antivirus Software Installation

Antivirus software is installed on all KTCH computers and servers. Virus update patterns are updated daily on the KTCH servers and workstations. Virus update engines and data files are monitored by the appropriate IT vendor who is responsible for keeping all virus patterns up to date.

> **Configuration -** The antivirus software is currently implemented by the IT vendor. Updates are received directly from the antivirus software and scheduled regularly.
> **Remote Deployment Configuration -** Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.
> **Monitoring/Reporting** – A record of virus patterns for all workstations and servers on the KTCH network may be maintained. Appropriate staff and/or business associates are responsible for providing reports for auditing and/or emergency situations as requested by KTCH.

New Software Distribution

All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. Appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained

from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the ITvendor. The software is often provided in an open distribution environment, special precautions must be taken before it is installed on KTCH computers and networks. These precautions include determining that the software does not, because of faulty design, "misbehave" and interfere with or damage KTCH hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a KTCH computer or network from another location are scanned for viruses immediately after being received.

Only approved staff may use USB devices as approved by the COO. All USB ports are inactivated until approval is received and will be activated by the IT vendor.
Computers shall never be "booted" from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not "bootable".

Retention of Ownership

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of KTCH are the property of KTCH unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging KTCH ownership at the time of employment. Nothing contained herein applies to software purchased by KTCH employees at their own expense.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.10

Subject: Telecommuting

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 9/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:

KTCH will consider telecommuting as a work arrangement in which some or all of the work to be performed by the employee is performed away from a designated work site when in the best interest of the organization.

PROCEDURE:

Provide standard procedures for the employees of Katy Trail Community Health concerning the practice of Telecommuting. While some positions within our organization may be appropriate to work away from the office (telecommuting), this may not feasible for all of our positions.

GENERAL:

Telecommuting may be proposed by either a supervisor or an employee. There must be an advantage to the organization in order for the request to be approved.

No particular positions have been designated as "telecommuting positions"; rather, certain positions may be suitable for performance outside the workplace, and in such a case, a supervisor may allow all or part of the duties of the position to be performed away from their normal worksite on a temporary, or an ongoing basis. However, no such arrangement is promised or guaranteed, and no particular duration of

telecommuting is guaranteed. If telecommuting is allowed for a position, it will last as long as it is appropriate for operational workflow and/or continuity of work in support of the KTCH mission.

Parts of this arrangement can be terminated at any time due to a change in circumstances-on the part of the employer or the employee personally-or due to a change in position description or negative impact on the organization or the employee's performance.

Child or adult daycare arrangements should not substantially change due to telecommuting. The intent is not to save employees the personal cost of daycare. Therefore employees who telecommute are strongly encouraged to maintain existing daycare arrangements to ensure an appropriate work focus.

The supervisor maintains the right to inspect the work area periodically during normal working hours. Employees who telecommute will receive 24-hours advance notice of such an inspection. An exception to the 24-hours' notice would be situations such as an imminent safety risk, information break, or a Health Information portability and Accountability Act (HIPAA) breach.

PROCEDURE:

- Employees wishing to be considered for working by telecommuting must apply for such consideration utilizing the Telecommuting Request/Authorization Form.
- The request must be granted or denied at senior leader level.
- If granted, the supervisor and the employee will work out the arrangement details.
- Such arrangement must be set forth in writing and signed by both the employee and the supervisor, using the Telecommuting Request/Authorization Form. Any remote worksite inspection must be done prior to the approval of the Telecommuting Request/Authorization Form.

GENERAL PROVISIONS:

This policy is not intended to be used for paid leave avoidance.

Telecommuting is a management tool, not an employee option.

Conditions of Employment- Telecommuting does not change the conditions of employment or required compliance with KTCH policies and procedures. The

employee will continue to comply with federal, state, and agency laws, policies, and regulations while working at the alternate work location.

Compensation and Benefits- An employee's compensation and benefits will not change as a result of telecommuting.

Hours of Work-The work hours of non-exempt telecommuting employees will not change from their approved work hour schedule regardless of work location. The recording of hours shall be recorded as usual through our Time and Attendance system. Should circumstances arise whereby the telecommuter cannot work at the alternate work location (i.e., loss of electricity, home emergencies, etc) the telecommuter must contact his/her supervisor and he/she may be required to report to their primary work location or applicable leave may be granted.

Attendance at Meetings- Unless other arrangements are made, telecommuters will be expected to attend all assigned office meetings related to the performance of their job, including those which would be held on a telecommuting day. Business meetings shall not be held at the alternate work location.

Workers Compensation Liability- KTCH may be liable for job-related injuries that may occur during an employee's established work hours in their alternate work locations. Accidents that occur at an employee's alternate work location may be subject to drug testing.

Any work related injuries must be reported to the employee's supervisor immediately. The employee shall agree to allow supervisors and/or an KTCH senior leader and/or designated representative to visit the alternative work location after any accident or injury occurs while working.

The employee understands that he/she remains liable for injuries or damage to the person or property of third parties or members of his family on the premises, and agree to indemnity and hold KTCH harmless from any all claims for losses, costs, or expenses asserted against KTCH by third parties or members of the employee's family.

Employee-Owned Equipment- When employees are authorized to use their own equipment KTCH will not assume responsibility for its cost, repair, or service.

Costs Associated with Telecommuting- KTCH is not obligated to assume responsibility for operating costs, home maintenance, or other costs incurred by employees in the use of their homes as telecommuting alternate work locations.

KTCH Information/Records- Employees must safeguard department information used or accessed while telecommuting. All department records, files, and documents must be protected from unauthorized disclosure or damage and returned safely to the primary workplace.

KTCH Owned Equipment- KTCH issued equipment is not to be used for personal purposes. The employee understands and agrees that they are to maintain the property in good condition. The employee is held financially responsible for damaged property.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.11

Subject: Transportable Media

Department(s) Affected/Distribution: All Departments

Effective Date: 9/24/15

Origination Approval: Mary Nell Strautman **Date:** 09/24/15

Approved By Board of Directors: Date(s): 9/24/15

Revision By: KTCH **Date:** 8/27/20

POLICY:
Katy Trail Community Health (KTCH) permits the use of transportable media in order to perform business operations. The purpose of this policy is to guide employees/contractors of KTCH in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from KTCH networks.

PROCEDURE:

Wireless Usage Standards

If your laptop does not have all of these software components, please notify your supervisor or the IT vendor so these components can be installed.

Use of Transportable Media

Transportable media included within the scope of this policy includes, but is not limited to SD cards, DVDs, CD-ROMs, and USB key devices.

Every workstation or server that has been used by either KTCH employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore, procedures must be carefully followed when copying data to or from transportable media to protect sensitive KTCH data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a KTCH employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common within KTCH. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of KTCH networks. Transportable media received from an external source could potentially pose a threat to KTCH networks. ***Sensitive data*** includes all human resource data, financial data, KTCH proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media, unless it is encrypted
- All USB keys used to store KTCH data must be issued by the Executive Administrative Assistant and/or the Privacy Officer. A checkout system of these company issued USB keys will be maintained by the Executive Administrative Assistant and/or the Privacy Officer and any missing USB keys will be reported to COO or CEO within 24 hours of the loss of such equipment. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by KTCH.
- Non-KTCH workstations and laptops may not have the same security protection standards required by KTCH, and accordingly virus patterns could potentially be transferred from the non-KTCH device to the media and then back to the KTCH workstation.

  Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.

- Data may be exchanged between KTCH workstations/networks and workstations used within KTCH. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:

  Data provided to auditors via USB key during the course of the audit.

Report all loss of transportable media to your supervisor or department head. It is important that the COO, and/or Privacy Officer are notified either directly from the employee or contractor or by the supervisor or department head immediately.

When an employee leaves KTCH, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

When no longer in productive use, all KTCH laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

Katy Trail Community Health
Information Technology Policies & Procedures

Policy/Procedure #: 3.12

Subject: Downtime Procedures

Department(s) Affected/Distribution: Clinical Staff

Effective Date: 4/10/18

Origination Approval: _____ **Date:** _____

Approved By Board of Directors: Date(s): _____

_____

Revision By: _____ **Date:** _____

Revision By: _____ **Date:** _____

POLICY: **The Electronic Health Record (EHR) software is used for data collection, order entry and clinical documentation. When the computer software is not functioning, the EHR administration will determine and announce when to implement downtime procedures. Downtime is defined as any time software is not functioning properly or is not available, whether scheduled or not scheduled.**

APPROVAL(S):

Chief Medical Officer (CMO)
Chief Dental Officer (CDO)
Chief Nursing Officer (CNO)

Down Procedure for Medical

PROCEDURE(S):

The following are the steps to be taken when the Electronic Health Record (EHR) is down for scheduled or non-scheduled downtime.

Scheduled Downtime:
For All Clinics – The day before Scheduled Downtime.

1. Print the Face sheet for all the patients that are on the appointment schedule for that day
2. Each clinic will be responsible for checking in, recording no-shows, or cancelling the patient 'encounter when they system becomes available

Additional Steps for EHR:

1. Print the most recent Visit Note for each patient scheduled to be seen the day of downtime; past medical history, surgical history, social history, family history, and vital signs.
2. Print the most recent laboratory results and diagnostic procedure results for the patient.

Day of Scheduled Downtime:

1. For future scheduling inform the patient the system is down. Request the patient's name, date of birth and a telephone number. After the system is available the patient will be called back with the appointment information.
2. Each clinic should have the following forms available
    a. Blank Demographic Sheets (new patient and established patient(s) packet)
    b. Established Patient Encounter Form (form attached)
    c. New Patient Encounter Form (form attached)
    d. Well Woman Exam Encounter Form (form attached)
    e. Care Coordination Encounter Form (form attached)
    f. Medical Lab Superbill (form attached)
    g. Return to Work/School Letter (form attached)
    h. Prescriptions Pads
3. Payment will be collected and a handwritten receipt will be issued to the patient.

When the System Becomes Available:

1. Enter/update ALL patient information in the HER
2. Post any patients received
3. Cancel/No Show all appropriate patient encounters
4. Call patients regarding the scheduling of future appointment times and dates.
5. Scan in consent forms signed by patient(s).
6. Scan Provider Orders into system
7. Scan in copies of prescriptions
8. Clinical staff should complete the patient visit information in the HER with all clinical information. Including updating current medication list and allergies

NON-SCHEDULED DOWNTIME FOR ALL CLINICS:

1. Have the following forms available and on hand.
    a. Established Patient (form attached)
    b. New Patient (form attached)
    c. Well Woman Exam (form attached)
    d. Care Coordination Form (form attached)
    e. Prescriptions Pads

2. A patient packet will be completed by all new Patients and a copy of the insurance card will be attached. For established patients, they will be queried as to where their insurance has changed and staff will obtain patient address and phone and write this information on the patient paper visit note. All other check-in processes remain the same.
3. Payment will be taken and a handwritten receipt will be issued to the patient.

When the system become available:

1. Follow steps as outlined under **"Scheduled downtime-When system becomes Available"**

DOWN TIME INSTRUCTIONS FOR DENTAL

If Dentrix is down:

1) Clean all dental operatories this includes; Wiping floor boards down, x-ray arms, base of chairs, counter tops, refill opti-cide, wash chairs, air spray the computer and keyboard.
2) Wipe down x-ray plate and carriers, wipe down pano machine.
3) Stock all operatories.
4) Stock sterilization room
5) Check inventory for reorder of supplies.
6) Work on dental assistant education.
7) Organize RCT material and composite material.
8) Clean storage area.
9) Clean laboratory.
10) Check paper towels and soap dispensers, cup dispensers.
11) Clean toys in waiting room.
12) Wipe down front office counter, equipment, dust bookcase, file cabinet.
13) If all else fails, go to your supervisor for instruction.