GEORGIA DEPARTMENT OF
COMMUNITY HEALTH

Policy and Procedure

Title:	Appropriate Use of Information Technology Resources	
Policy #:	419	Pages: 13
Document Type:	Technology & Security Standards	
Effective Date:	May 16, 2000	Revision Date: August 16, 2012
POC for Changes:	Division of Information Technology, OIS	
References:	(1) HIPAA Final Security Rule: "Security Standards for the Protection of Electronic Protected Health Information", 45 CFR Part 160 and Part 164, Subparts A and C. (2) State Enterprise Information Security Policies and Standards. (3) National Institute of Standards and Technology (NIST) Risk Management Framework developed in accordance with the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. (4) DCH Policy No. 410, Standards of Conduct. (5) DCH Policy No. 418, Use of State Property, Fax Equipment, Pagers, Vehicles, and Other Resources. (6) DCH Policy No. 435, Managing Authorization, Access and Control to Information Systems and Request for Network Access Form.	

I. Purpose

The DCH Division of Information Technology seeks to promote the efficient use of information technology, and to promote the use of technology to deliver public services in a way that works better, costs less and is capable of serving our health plan members' and other customers' needs appropriately and effectively. The DCH Division of Information Technology also establishes DCH information security policy and procedures.

Information Technology (IT) Resources are provided to authorized individuals to facilitate the efficient and effective performance of their duties for the Georgia Department of Community Health (DCH). The IT Resources provided to individuals by DCH or at the request or direction of DCH, in order for those individuals to provide services for DCH, are referred to in this policy and procedure as "DCH IT Resources." Access to DCH IT Resources is limited in accordance with DCH Policy 435.

The purpose of this policy is to establish guidelines for the use of all DCH IT Resources, including those IT Resources managed by the Georgia Technology Authority and delivered by the State's IT Enterprise Service Providers - IBM and AT&T. These guidelines define appropriate business use of DCH IT Resources and establish requirements for protecting the privacy and security of electronic DCH information.

This policy also establishes required and appropriate information security controls that ensure the confidentiality, integrity and availability of DCH information and information systems and the privacy and security of DCH's electronic Protected Health Information.

II. Scope

This policy applies to all individuals who utilize, possess, or have access to DCH IT Resources in order to perform services for DCH as an employee or as a non-employee DCH worker "on assignment" with DCH (such as temporary staffing agency employees and independent contractors). These individuals are called "DCH IT Users" in this policy and procedure. See DCH Policy 435 for information about access to DCH IT Resources by other individuals pursuant to contractual agreements.

III. Definitions

"**Document**" refers to any kind of file that can be read on a computer screen as if it were a printed page, including files read in an Internet browser, any file meant to be accessed by a word processing or desk-top publishing program or its viewer, or the files prepared for reading by other software or other electronic publishing tools.

"Display" includes monitors, flat – panel active or passive matrix displays, LCD's, projectors, televisions and virtual-reality tools.

"Electronic media" means (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Certain transmissions, including paper via facsimile, and voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

"Electronic protected health information" ("E-PHI" or **"ePHI")** means protected health information that is transmitted by electronic media or maintained in electronic media.

"Electronic mail" ("e-mail" or **"email")** is a method of composing, sending, storing, and receiving messages over electronic communication systems or Email Systems. The term e-mail applies both to the Internet e-mail and to intranet systems allowing users within one agency or organization to send messages to each other.

"Email Systems" are software and hardware systems that transport messages from one computer user to another. E-mail systems range in scope and size from a local email system that carries messages to users within an agency or office to an e-mail system that sends and receives messages around the world over the Internet.

"E-mail messages" are electronic documents created and sent or received by a computer via an e-mail system. This definition applies equally to the contents of the communication, the transactional information, and any attachments associated with such communication. E-mail messages are similar to other forms of communicated messages, such as memoranda and letters.

"Encryption" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"GETS" means the Georgia Enterprise Technology Services IT privatization contract awarded by the Georgia Technology Authority to IBM and AT&T to provide consolidated IT Infrastructure and Network Management Services designed to ensure a stable, robust, secure, cost-effective, and centralized IT Platform and Service delivery model for the State of Georgia.

"**Graphics"** includes photographs, pictures, animations, movies, or drawings.

"Individually Identifiable Health Information" means information or data, including demographic information collected from an individual, that (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (3) That identifies the individual; or (4) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Information Technology Resources" or "IT Resources" means hardware, software, and communications equipment, including, but not limited to, personal computers, mainframes, networks, servers, portable computers, peripheral equipment, cell phones, personal digital assistants (PDA's), wireless communications, facsimile machines, technology facilities including but not limited to, data centers and dedicated training facilities and other relevant hardware and software items as well as personnel tasked with the implementation, and support of technology. The IT Resources provided to individuals by DCH or at the request or direction of DCH, in order for those individuals to provide services for DCH, are referred to in this policy and procedure as "DCH IT Resources." All individuals who utilize, possess, or have access to DCH IT Resources in order to perform services for DCH as an employee or as a non-employee DCH worker "on assignment" with DCH (such as temporary staffing agency employees and independent contractors) are referred to as "DCH IT Users."

"Key Size" specifies the number of repetitions of transformation rounds that convert the input, called the plain text, into the final output called the cipher text.

"Limited Use" is defined as ten (10) minutes or less of personal use of the Internet during breaks or lunch.

"Protected Health Information" or "**PHI**" means Individually Identifiable Health Information that is (1) Transmitted by electronic media; (2) Maintained in electronic media; or (3) Transmitted or maintained in any other form or medium

"Removable Media" means portable USB-based memory sticks, also known as flash drives, thumb drives, jump drives, key drives, or writable and rewritable DVDs and CDs, and external hard drives.

IV. Policy

The DCH Division of Information Technology and its Office of Information Security shall ensure that GTA and the GETS Infrastructure and Network Management Service Providers take the appropriate steps, including the implementation of strongest-available and practicable encryption, user authentication, and virus protection measures, to mitigate risks to the privacy and security of DCH data and information systems associated with the use of DCH IT Resources by DCH IT Users.

DCH IT Users must protect DCH IT Resources from unauthorized access, misuse, and loss. DCH IT Users must protect the privacy and security of DCH IT Resources over which they have control or to which they have access. It is the responsibility of the User to manually lock their computer screen before leaving it unattended for any period of time. The DCH Division of Information Technology, Office of Information Security shall ensure that all DCH IT Users receive training necessary for them to protect the confidentiality, integrity, availability, privacy and security of the information over which they have control, or to which they have access, as a result of their use of DCH IT Resources. This training must be provided upon receipt of access to DCH IT Resources and on an as needed basis. In addition, this training must be provided on a regularly scheduled basis (annually or as close to annually as practicable).

V. Procedures

All DCH IT Users must satisfactorily complete initial Information Security Awareness Training and HIPAA Privacy/Security Training Programs and annual "refresher" training. Satisfactory completion of training will be demonstrated by the DCH IT Users providing correct answers to all quiz questions. Training materials and documentation of completion of training will be retained by the DCH Office of Human Resources for all DCH employees, and will be retained by the DCH HIPAA Privacy and Security Officer for all DCH IT Users who are not DCH employees. All DCH IT Users must comply with the provisions of this policy and procedure, including the attached DCH Information Technology User Agreement, and any guidelines set forth in current training materials. Non-compliance with this policy and procedures, the attached DCH Information Technology User Agreement or guidelines set forth in current training materials will subject DCH IT Users to disciplinary action, up to and including termination, in accordance with applicable DCH Policies and Procedures, such as DCH Policy 911 (Sanctions).

DCH IT Users that become aware of any incident that threatens the privacy or security of DCH IT Resources should immediately report the existence of such incident to their immediate Supervisor, the Agency Information Security Officer (see Section XV for contact information), or in the case of security incidents involving PHI, the HIPAA Privacy and Security Officer (see Section XV for contact information).

Such incidents include, but are not limited to:

(1) Loss, theft, or destruction of a DCH-issued desktop or laptop, regardless of whether the information is believed to be encrypted or otherwise safeguarded;

(2) Loss, theft, or unintended destruction of any Media (including thumb drives, flash drives, CD's, DVD's, external hard drives, etc.) that contains DCH information, regardless of whether the information stored in the Media is believed to be encrypted or otherwise safeguarded;

(3) Loss, theft, or destruction of a DCH issued wireless or mobile device; including, but not limited to a BlackBerry, iPad, or other PDA, regardless of whether the information contained in the device is believed to be encrypted or otherwise safeguarded.

(4) Fraudulent or unauthorized access to DCH information systems, including, but not limited to, those managed by GTA/GETS.

(5) Sharing of passwords.

(6) Improper use of GTA/GETS Managed e-mail services or Internet access.

(7) Threats or damage to DCH employees, facilities, or systems.

DCH IT Resources are to be used only in a manner consistent with the goals and objectives of DCH, and are to be used to accomplish work-related assignments. DCH IT Users who divert DCH IT Resources for personal gain will be required to reimburse DCH and will be subject to other appropriate disciplinary action, including but not limited to termination.

Except as described below, DCH IT Users are not allowed to move any DCH IT Resource from its approved location. For example, the approved location for a DCH IT User's desktop computer is his or her office or cubicle. The approved location for a printer, fax machine, or copier is the location approved by the DCH Support Services.

(1) DCH IT Users may carry portable DCH IT Resources issued to them (such as DCH issued laptops, blackberries, iPads, or other PDAs) with them, as long as they maintain sole possession of these DCH IT Resources and secure them in accordance with applicable DCH policies and procedures and guidelines from current training.

(2) DCH IT Users may relocate other DCH IT Resources only with written approval of their Division, Office, section, or unit director and written approval of DCH Support Services or Division of Information Technology, whichever is responsible for issuing that type of DCH IT Resource.

(3) DCH IT Users who work for GETS Service Providers, DCH Support Services, or in the Division of Information Technology may relocate DCH IT Resources as necessary to perform their work of issuing DCH IT Resources. They shall follow applicable internal procedures to ensure that all DCH IT Resources are inventoried and that access to DCH IT Resources is provided in accordance with the requirements of Policy 435.

(4) DCH IT Users may not connect a personal flash drive, CD, DVD, or external hard drive to a DCH computer without written approval by a supervisor and the IT Department.

Guests may use their own portable media devices on their own computer or a loaner laptop provided by DCH IT but it should not be connected to the DCH network. If a guest needs internet access, DCH IT must set up an external internet connection.

VI. Software Licensing

The State's GETS Service Provider managed networks and Department Software Applications, and software are to be used responsibly by all DCH IT Users. DCH IT Users must comply with local, State, and federal laws related to copyrights, software licensing, and restrictions regarding the transmission of threatening or obscene materials. All computer software installed on DCH computers and systems must be licensed as required by the software manufacturer. All DCH IT Users must follow and abide by commercial licensing laws and requirements.

VII. Secure Password Standards

Passwords are essential in protecting State networks, systems, and sensitive agency data. Individual passwords are established and maintained by each employee for access to critical Information Technology business systems and software. Network, system, and application user accounts must be assigned to specific individuals and not assigned to anonymous user accounts, groups, departments, job functions, etc. DCH IT Users have a duty and responsibility to ensure that passwords remain private and confidential. Sharing LAN network, system, application, and/or screen saver passwords with any other person is prohibited. Passwords prevent unauthorized access to various common directories on the network and the email system, as well as possibly access to external computer systems. DCH IT Users may give specific individuals access to their files and email by requesting such access through the Division of Information Technology. Strong Password Standards, as defined by State Enterprise Information Security Policies and Standards, must be followed for access to any State LAN network, system, or business software application.

Strong passwords include the following characteristics.

(1) They must be at least eight characters in length; and

(2) They must include three of the following four characters: and
- English upper case (A-Z)
- English lower case (a-z)
- Numbers (0-9)
- Non-alpha special characters ($, %,^)

(3) They must not contain the user's name; or

(4) They must not contain part of the user's full name.

VIII. Data Encryption Standards

All files, information or data containing ePHI shall be encrypted (utilizing the strongest available encryption technology and key size) while stored on removable Media and during transmission outside of DCH's network. DCH IT Users must follow the guidelines of current training materials regarding encryption of ePHI and methods for securely transmitting ePHI. Information and data containing ePHI shall also be encrypted before being backed-up to other data storage devices or Media. All ePHI data residing on DCH- issued desktop computers, portable computing devices (laptops) or other mobile computing devices shall be encrypted utilizing full-disk encryption technology. DCH IT Users shall not store any files or information containing ePHI to any removable Media, such as Flash Drives, CD's, DVD's, or external Hard Drives, etc. unless: (1) the DCH IT User's supervisor has provided written approval for the DCH IT User to store the files or information on the removable Media, and (2) the DCH IT User saves the files to a DCH issued removable Media device, and (3) the information or data is encrypted while stored on the device. The encryption protocols utilized by DCH shall comply with the most current National Institute of Standards and Technology (NIST), FIPS-197 Advanced Encryption Standard (AES).

DCH Division of Information Technology is responsible for ensuring encryption of ePHI "at rest" while stored on non-portable storage devices and backup storage devices to the extent practicable. As required by law, if encryption is not practicable, DCH Division of Information Technology shall maintain documentation of the reasons why encryption is not practicable as well as documentation that alternative physical, technical and administrative controls are being implemented to protect the privacy and security of the unencrypted ePHI. DCH IT Users are responsible for ensuring that ePHI is encrypted during transmission and during storage on portable Media devices. DCH IT Users should always utilize the strongest encryption protocol available when configuring wireless routers or networks at home.

IX. Saving ePHI

DCH IT Users shall save all files, information and data containing ePHI in a manner that restricts access to the ePHI to those who require access to it (either for current needs or for business continuity purposes), and that complies with applicable policies and procedures and current training guidelines.

Whenever possible, ePHI shall be saved to a DCH server, which is backed up, to prevent inadvertent or unauthorized destruction.

All ePHI you save must be protected from access by others who do not need it. Documents and files containing ePHI that may be accessed by anyone in your Division must be saved in your Division folder on the O:\Drive (or on your Division server). Only employees assigned to your Division may see files in your Division folder. Documents and files containing ePHI that may only be accessed by certain people in your Division must be saved in a Restricted sub-folder in your Division folder (created by IT).

IX. Malware and Anti-Virus Software

The GTA/GETS Infrastructure Service Provider has installed anti-virus software on the State network and information systems to detect and "sanitize" malware and virus programs that may be introduced. Accordingly, and for security reasons, the anti-virus software programs must not be disabled. Downloading and Installing software from outside the office or from the Internet on State desktop or laptop hard drives without written approval from the Division of Information Technology is strictly prohibited. This is necessary due to the limited availability of hard disk space, the danger of importing computer SPAM and viruses, and the software licensing issues mentioned above. These SPAM e-mails can redirect a user's Web Browser to virus infected Web Sites which can install malicious software on State computers and networks. However, these devices cannot block all e-mails containing such Links. DCH IT Users should never click on Web Links in e-mails from unknown or suspicious sources. When in doubt, contact the Division of Information Technology Help Desk or the Agency Information Security Officer.

X. Virus protection must be running on your computers. Always restart your machine to pick up the latest patches and virus definitions. NEVER open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash. Delete spam, chain, and other junk email without forwarding. Do not download files from websites unless absolutely necessary to accomplish your work. Never download freeware onto your workstation. If your computer detects a virus, stop using the computer and notify the DCH IT Help Desk or call the GETS help desk at 877-482-3233 immediately.

Personal information technology resources may never be connected to DCH IT Resources. DCH Management reserves the right to examine and review content on personal information technology resources reasonably believed to have been connected to DCH IT Resources or to contain DCH information. Examples include but are not limited to items such as personal USB drives, personal external hard drives, personal CD's, DVDs, personal laptops or any other personal computing device that has the ability to connect with DCH Information Technology Resources.

XI. Internet and E-mail Use

Personal

The State's Infrastructure Service Providers provide Internet access and e-mail addresses as required by DCH to DCH IT Users for the efficient and effective performance of their duties for DCH. Internet access is provided to allow business-related research and access to information needed to facilitate business communication with customers, vendors, colleagues and others receiving services from, doing business with, or seeking information from DCH. Computer equipment and other IT Resources required for Internet access and e-mail accounts are provided at significant cost to the State, and as with other State property, DCH IT Users must ensure that such resources are not misused. Although valuable business tools, Internet and e-mail access are considered privileges, and as such DCH reserves the right to revoke access to either or both for inappropriate usage or take any other appropriate disciplinary action, including termination.

Examples of inappropriate Internet use include, but are not limited to, the following:

(1) Private or personal for-profit business activities. This includes Internet use for private purposes such as private advertising of products or services, or any activity meant to foster personal gain.

(2) For profit business transactions or unauthorized not-for-profit business activities.

(3) Conducting any illegal activities as defined by federal, State, and local laws or regulations.

(4) Political or religious causes.

(5) Accessing or downloading sexually explicit or pornographic material.

(6) Accessing or downloading material that could be considered discriminatory, offensive, threatening, harassing, or intimidating, including ethnic or racial slurs or jokes.

(7) Gambling.

(8) Uploading or downloading commercial or agency software in violation of copyright or trademark.

(9) Downloading any software or electronic files without approval from the IT Division or ensuring that DCH provided virus protection is active.

(10) On-line shopping and auctioning.

(11) Accessing Web chat sites and dating sites.

Examples of appropriate Internet use include the following:

(1) Job-related research.

(2) Access to federal, State, or local government Internet sites.

(3) Access to sites related to professional organizations or other professional development information.

(4) Limited use during personal time (i.e., breaks and lunch).

Information, data and files composed, transmitted, or received on DCH IT Resources, including Internet data and e-mail messages, are subject to disclosure under the Georgia Public Records Act (http://sos.georgia.gov/archives/who_are_we/rims/best_practices_resources/open_records_act.htm). DCH IT Users should ensure that all data accessed with or stored on DCH IT Resources is appropriate, ethical and lawful. E-mail users should be mindful of how they represent themselves, since any message or data sent through the e-mail system clearly identifies the message as coming from DCH and could be interpreted as a Statement of DCH opinion, position or policy. Additionally, data that is composed, transmitted, accessed or received via State Internet resources must not contain content that may be considered discriminatory, offensive, threatening, harassing, intimidating, or disruptive.

Email is NOT the same as a letter sent through the normal mail. Your messages are "written" on the electronic equivalent of postcards. What does this means? Anyone can look at your message. Do not email ePHI to a non-DCH email account, unless the email has been encrypted. If you need to email ePHI to perform your job, please use Voltage ("Send Secure") encryption or contact your local support team for instruction. Do not use non-DCH email such as Web Mail (like gmail, hotmail, yahoo, etc.) to conduct business or send ePHI. Secure FTP (SFTP) may be used to send ePHI outside of DCH. Contact the IT Help Desk for instructions.

Before you send an Email that contains PHI: check all addresses for accuracy, use "Send Secure", and consider using an Email delay feature that allows you to stop an Email from going out if you accidentally hit "Send" instead of "Send Secure". MOVE Emails that contain attachments with PHI to folders on your P: Drive. Sending ePHI Out of DCH.SECURE FTP (File Transfer Protocol) is the BEST way to exchange large files containing ePHI. If you regularly need to get or send a large file containing ePHI outside the DCH network, contact the IT Department to set up Secure FTP (SFTP). "Send Secure" email may be used to send smaller files. Send Secure will encrypt the message and the file. If Send Secure is not available, you may email a message that does not contain ePHI and attach an encrypted file. Excel, Access, Word, PDF all have instructions for encrypting the document. Encryption is different from "password protection". It is YOUR responsibility to ask the ISO if you do not know how to encrypt a file. The password to open the encrypted file must be a strong password and must be sent using "Send Secure" email or shared by phone, fax or mail. If you regularly need to email ePHI to a vendor, contact the ISO to make sure that DCH has a secure, encrypted "tunnel" to the vendor. If a secure tunnel exists, "Send Secure" is not necessary, but is still the best choice. Always email to the vendor contact's work email. The secure tunnel only works between your DCH email address and the vendor's work email address. It is ok to email ePHI to a DCH worker at the DCH email address if necessary. Only email the minimum necessary ePHI. Only include authorized individuals on the email. Review any email before forwarding to make sure you are not sending ePHI to someone who does not have a need to see it. Any large file containing ePHI should be saved in a Restricted Folder. Email the path to the folder instead of the file itself. Never send ePHI to any personal email address without supervisor approval. ePHI may only be sent for business purposes. Email is usually not a good way communicate ePHI to customers. All email must contain the following statement: Reader Advisory Notice: Email to and from a Georgia state agency is generally public record, except for content that is confidential under specific laws. Security by encryption is applied to all confidential information sent by email from the Georgia Department of Community Health.

XII. Monitoring Use of DCH IT Resources

While DCH respects the privacy of DCH IT Users, ensuring compliance with this policy and procedure is of utmost importance. Therefore, DCH reserves the right to retrieve and read content or data including but not limited to any data composed on DCH IT Resources, transmitted using DCH IT Resources, received through DCH on-line connections, or stored on DCH IT Resources, to monitor Internet sites visited and access attempts, and provide information relevant to an investigation of suspected violations of DCH policies and procedures or laws. Inappropriate Internet or e-mail usage can expose DCH to significant legal liability and reflect negatively on DCH. The State's Infrastructure Service Provider has installed software to prevent access to many objectionable Internet Web content and to monitor State Internet access.

The Division of Information Technology may review and document Internet activity, email usage or usage of other DCH IT Resources. DCH IT Users should be aware that any information accessed, downloaded, or transmitted may be reviewed by information security staff, the Office of Inspector General, and the HIPAA Privacy and Security Officer, as needed, and DCH management will be notified if a DCH IT User's use of DCH IT Resources violates DCH policies or procedures or laws, such as by repeatedly attempting to reach blocked Internet sites, frequently visiting non-work related sites, or emailing DCH information to personal email accounts. When using DCH IT Resources, including, but not limited to e-mail and Internet, DCH IT Users are consenting to the monitoring of their use and have no reasonable expectation of privacy in the use of the DCH IT Resources. Failure to comply with this policy and procedure may result in disciplinary action, up to and including termination from employment.

XIII. Policy and Procedure Revisions

The Chief Information Officer (or his designee) is responsible for reviewing, maintaining and updating this policy and procedure, the attached DCH Information Technology User Agreement, and Information Security training materials as necessary and appropriate.

XIV. Dissemination

This policy and its attachments must be reviewed and acknowledged by all DCH IT Users during Orientation or upon being provided with access DCH IT Resources, whichever comes first. In addition, the policy will be posted on the DCH Intranet Web Portal and made available to all DCH IT Users. Any revisions to the policy and its attachments will be communicated to all DCH IT Users and knowledge of the policies and procedures must be acknowledged, in writing, by all DCH IT Users at least annually.

XV. Information Security and HIPAA Privacy and Security Contacts

Agency Information Security Officer:
Sherman Harris, ISO
Phone: 404 656-9653
E-Mail: sheharris@dch.ga.gov

Agency HIPAA Privacy & Security Officer:
Alison Earles, Attorney
Phone: 404 656-0412
E-Mail: aearles@dch.ga.gov

Division of Information Technology Help Desk
Phone: 404 657-7171
E-Mail: helpdesk@dch.ga.gov

Appendix A
Information Technology User Agreement

By accessing DCH IT Resources, DCH IT Users agree to maintain the privacy, security, confidentiality and integrity of State and DCH data and computing resources over which he or she has control or to which he or she may have access. DCH IT Users must review this policy and procedure and the current Information Security Training materials and agree to comply with them by signing the DCH Policies and Procedures Acknowledgement Form upon start of work and annually thereafter.

Use of Information Technology Resources

(1) DCH IT Users shall not attempt to circumvent IT privacy or security safeguards, and any such attempts may lead to revocation of a DCH IT User's access and may result in disciplinary action, as appropriate.

(2) DCH IT Resources, including e-mail accounts and Internet access, may be monitored at anytime without additional prior notice, and if such monitoring reveals violations of State or DCH policies, the Chief Information Officer (CIO) or his designee and the Office of Human Resources will be notified and appropriate sanctions will be applied. If such monitoring reveals misconduct or illegal behavior, the activity will be referred to the DCH Office of Inspector General for internal investigation and further action, as needed.

(3) DCH IT Users shall not add any network equipment or infrastructure to the State network except as authorized by Division of Information Technology or GTA/GETS Service Provider management as part of a DCH IT User's job responsibilities. The DCH IT User's supervisor or contracted business program sponsor must inform the Division of Information Technology when he or she no longer requires access to DCH IT Resources, in accordance with DCH Policy 435.

(4) DCH IT Users shall not relocate computing equipment, workstations, printers, scanners, etc., without proper authorization or assistance from the appropriate Division of Information Technology support staff.

(5) DCH IT Users shall only physically connect to the State's Infrastructure network using DCH IT Resources.

(6) DCH IT Users shall not disclose ePHI in e-mail unless the e-mail is encrypted as described in current training guidelines.

(7) DCH IT Users shall use their best efforts to send only e-mail content that is appropriate for transmission in that media, ensuring messages are professional, current, accurate, and factual.

(8) DCH IT Users will be mindful of the right of any person to inspect and copy emails upon request, under the State of Georgia public records law (http://sos.georgia.gov/archives/who_are_we/rims/best_practices_resources/open_records_act.htm).

(9) DCH IT Users shall take reasonable and appropriate steps to protect DCH IT Resources from loss, damage, or theft and understands that failure to do so may result in disciplinary action.

(10) DCH IT Users shall not attempt to introduce a computer virus or other malicious program code into State networks, systems, or software.

(11) DCH IT Users shall not attempt to bypass, strain, or test security safeguards or mechanisms, unless authorized as required by specific job responsibilities.

(12) DCH IT Users shall comply with guidelines set forth in current Information Privacy and Security training materials.

Software Licensing and Intellectual Property

DCH IT Users requiring additional computer software, equipment, or media that was not originally issued, shall contact the Division of Information Technology Help Desk to request the required resources. The Division of Information Technology will ensure that the appropriate software licensing and agreements are obtained. DCH IT Users shall not download, use or connect any unauthorized software, freeware, adware, shareware, or hardware onto any State network, system, workstation, wireless/mobile device, nor violate software copyright, trademark or licensing restrictions.

Approved by:	**Date:** 8/20/12