Georgia Department of Community Health

Information Technology Policy: **Use of State Computers and the Internet**	**Policy No.** 419
Effective Date: May 16, 2000 **Revised Date:** October 22, 2008	**Page** 1 of 11

References:
1. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, Privacy Rule and Security Rule
2. DCH Policy No. 418, Use of State Property, Fax Equipment, Pagers, Vehicles, and Other Resources
3. DCH Policy No. 410, Standards of Conduct
4. Georgia Technology Authority (GTA) Enterprise Security Policies

I. Purpose

The purpose of this policy is to establish guidelines for the use of computer hardware and software and appropriate business usage of Internet access and electronic mail (e-mail) accounts provided by the Georgia Department of Community Health (DCH). The privacy and security of protected health information are high priority concerns of DCH. Accordingly, the following policy and procedures are intended to support the Department's safeguards of privacy and security. DCH seeks to promote the efficient use of resources and to promote the delivery of public services through the use of an information technology (IT) enabled system that works better, costs less and is capable of serving our members' and other customers' needs appropriately.

II. Scope

This policy applies to all employees of DCH, attached agencies, temporary agency personnel, contractors, vendors, and any other persons who utilize, possess or have access to DCH computer equipment, DCH-provided Internet access and electronic mail accounts.

III. Definitions

For purposes of this policy, the following terms mean:

A. **"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.

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

C. **"Electronic media"** means (1) Electronic storage media including memory devices in computers (hard drives) and any removable or 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.

D. **"Electronic protected health information"** or **"E-PHI"** means protected health information transmitted by electronic media or maintained in electronic media.

E. **"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.

F. **"E-mail 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.

G. **"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.

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

I. **"Individually identifiable health information"** means information, 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; and

(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

(i) That identifies the individual; or
(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

J. **"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, 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.

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

L. **"Protected health information"** or "**PHI**" means individually identifiable health information that is:

(i) Transmitted by electronic media;
(ii) Maintained in electronic media; or
(iii) Transmitted or maintained in any other form or medium.

M. **"User" or "IT User"** means employees, contractors, vendors, or any other individuals who are granted access to a DCH information technology resource.

IV. Policy

DCH shall take 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 information technologies. DCH IT resources, including data, hardware and software, will be protected from unauthorized access, misuse, or loss. Individual IT users must take steps to help protect the privacy and security of IT resources over which they have control or to which they have access. Individuals who use DCH IT resources will be trained in the DCH information privacy and security program. Confidential information, including protected health information, must be protected from unauthorized disclosure, modification, use, or destruction. Safeguards must be maintained to ensure that its integrity, confidentiality, and availability are not compromised.

V. Procedures

The entire DCH workforce must satisfactorily complete the Information Security Awareness Training and Privacy Training Programs. Satisfactory completion will include testing and scoring on the tests a minimum of eighty percent (80%) correct answers to the test questions. Training materials, tests and scores will be retained by the DCH Compliance Section in the General Counsel Division as documentation of the training.

IT Users must comply with the provisions of the IT User Agreement. Noncompliance with this policy and the attached agreement will subject workforce members to disciplinary action, up to and including termination, in accordance with the DCH Privacy Policy for Sanctions and with the DCH Policy on Progressive Discipline. The sanctions applied, if any, will be in proportion to the severity of the noncompliance and the risk of harm attributable to the individual's noncompliance.
IT Users that become aware of any incident that threatens the Privacy or Security of DCH IT resources, including but not limited to information systems, databases, computer networks, premises, assets, or personnel should immediately report the incident to their immediate supervisor and to the Director of Compliance in the General Counsel Division.

Such incidents include, but are not limited to:

- Loss or theft of a DCH-issued laptop or a personal laptop that contains confidential or protected health information, regardless of whether the information is believed to be encrypted or otherwise safeguarded;
- Loss or theft of any portable media that contains confidential or protected health information, regardless of whether the information is believed to be encrypted or otherwise safeguarded;
- Loss or theft of a DCH issued personal digital assistant (PDA), including a BlackBerry, PalmPilot or a personal PDA that contains confidential or protected health information, regardless of whether the information is believed to be encrypted or otherwise safeguarded;
- Fraudulent access to DCH information systems, unauthorized access or use of DCH resources or services, shared or compromised passwords, or improper use of DCH email or Internet access;
- Threats or damage to DCH employees, facilities, or systems.

VI. Maintenance of Policy

The Chief Information Officer or his designee is responsible for reviewing, maintaining and updating this policy and the IT User Agreement as needed.

VII. Dissemination and Training

This policy will be disseminated to employees during New Hire Orientation and upon an individual's being provided with access to the DCH network, whichever comes first. In addition, the policy will be posted on the DCH Intranet and emailed to all employees. The IT Division will ensure delivery of mandatory training on the policy for the entire workforce and will ensure annual training on the policy for all employees. As an employee's duties and responsibilities or access to information systems changes, the IT Division will ensure that appropriate role-based and access-based training about the use of IT resources is provided to each such employee.

VIII. Computer Equipment

A. The computer resources are to be used only in a manner consistent with the goals and objectives of the Department.

B. State computers and equipment are to be used to accomplish work-related assignments. Employees who divert state property or resources for personal gain will be required to reimburse the Department and will be subject to other appropriate disciplinary action. State computers and equipment are to be used for state business only.

C. Employees must obtain written approval from their division, office, section, or unit director, as appropriate, before removing computer equipment from offices of the Department. The approval must show decal number, make, model, and serial number of the computer equipment being removed. Employees located at the 2 Peachtree Street building are required to submit the supervisory approval to the Information Technology Infrastructure Services (ITIS) Section in order to obtain a *PROPERTY REMOVAL FORM.*

D. For employees who are assigned a laptop or other computer equipment for regular use, one *PROPERTY REMOVAL FORM* may be issued to the employee for the estimated period of time, up to one year, that the employee exclusively will be using the equipment. Upon the expiration of the time authorized, a new form will be completed as needed for continued exclusive use of the equipment.

IX. Licensing

A. The network(s) are to be used responsibly by all DCH employees and vendors. The users of the network are responsible for respecting and adhering to local, state, and federal laws including those laws related to copyrights, software licensing, and transmission of threatening or obscene materials.

B. All computer software installed on departmental computers must be licensed as required by the software manufacturer. All DCH employees will follow and abide by commercial licensing laws and requirements.

X. Security of Passwords and Network Data

A. Individual passwords are established by each employee for access to the network(s). Passwords shall remain private and confidential. Sharing network and/or screen saver passwords with any other person is prohibited. Passwords prevent unauthorized access to the various common directories on the network and the e-mail system, as well as possible access to external entity computer systems.

Users may give specific individuals access to their files and e-mail by requesting such access through the Division of Information Systems.

B. Strong passwords must be used. Strong passwords are defined as having the following characteristics:

- ☐ Are at least eight characters in length.
- ☐ Contain characters from at least three of the following four types of characters:
  - ☐ English upper case (A-Z)
  - ☐ English lower case (a-z)
  - ☐ Numbers (0-9)
  - ☐ Non-alpha special characters ($, !, %, ^, ...)
- ☐ Must not contain the user's name
- ☐ Must not contain part of the user's full name

C. The Department has installed anti-virus software on the network(s) to detect and "clean" any virus introduced. Accordingly, for security reasons, the anti-virus program must not be disabled.

D. Installing software and screen savers other than DCH-approved software and files on PC hard drives is prohibited because of the limited hard disk space, the danger of importing computer viruses, and the software licensing issues mentioned above. The prohibition includes music files, pictures, file sharing software and other programs and applications outside of the software, programs and applications installed by or with the approval of the IT Division. At no time may a user install software on the network server, as this will increase the danger of introducing and spreading viruses to the network.

E. The Department may issue laptop computers or other computer hardware to staff. If issued a laptop or other equipment, staff assumes responsibility for the safety and security of the equipment and should follow procedures outlined in Sec. VIII. for removal of equipment from the DCH offices.

XI. Use of the Internet and E-mail

A. DCH will provide Internet access and e-mail addresses as necessary to employees for the efficient and effective performance of their duties. Internet access is provided to facilitate business-related research and access to information and to enhance communication with customers, vendors, colleagues and others receiving services from, doing business with, or seeking information from DCH employees.

B. Computer equipment and other resources required for Internet access and e-mail accounts are provided to employees at significant cost to the State, and as with other state property, employees 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.

C. Data and files composed, transmitted, or received on DCH equipment, including Internet data and e-mail messages, are subject to disclosure under the Georgia Public Records Act upon request. Employees should ensure that all data accessed with or stored on DCH equipment is appropriate, ethical and lawful. E-mail users should be careful about how they represent themselves, since any message or data sent through the DCH 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 DCH Internet resources must not contain content that may be considered discriminatory, offensive, threatening, harassing, intimidating, or disruptive to any employee or person.

D. Under no circumstances should DCH equipment or resources be used for: business or solicitations related to commercial ventures, religious or political causes, or any matter related to outside organizations, illegal activity, downloading or distributing pirated software, data or malicious program code (viruses), downloading personal software, files or programs or any other activity that would reflect discredit on DCH.

E. The use of state-provided Internet access imposes certain responsibilities and obligations on users and is subject to state government policies and state and federal laws. As a condition of being granted Internet access by DCH, each employee must comply with this policy and refrain from inappropriate use at all times, including access during breaks or outside of regular business hours.

F. Examples of <u>appropriate</u> Internet use include the following:

1. Access to federal, state, or local government Internet sites;

2. Job-related research; and

3. Access to sites related to professional organizations or other professional development information. Additionally, employees may make <u>limited use</u> (See definition of "limited use") of the Internet on personal time at work consistent with the rest of this policy. Personal time includes breaks and lunch.

G. <u>Inappropriate</u> Internet use includes, <u>but is not limited to</u>:

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

2. 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 ensuring that DCH-provided virus protection is active;

10. On-line shopping and auctioning;

11. Accessing Web chat sites and dating sites; and

12. Downloading any software or programs from the Internet onto a DCH computer without express approval by the Division of Information Systems.

H. Employees are also restricted from downloading trial versions of software unless prior arrangements are made with the ITIS Section.

I. Personal Use of the Internet and E-mail

1. DCH acknowledges that occasional personal use of Internet connectivity may occur. Any such use must be brief and infrequent, and limited to lunch and break periods or other non-work time. Examples of appropriate personal usage include: checking weather forecasts, accessing traffic reports, accessing deferred compensation or other benefit information. Employees are reminded that **inappropriate** use of DCH Internet access as defined above **is prohibited at all times**.

2. The e-mail system may not be used to distribute chain letters or other personal solicitations.

3. Unnecessary Internet usage causes network and server congestion, slows other users, takes away from work time, and could overburden other shared resources. Because of this, accessing/ downloading audio or video files is strictly limited to business purposes only.

XII. Internet and E-mail Usage Monitoring

A. While DCH respects the privacy of employees, ensuring compliance with this privacy and security policy is of utmost importance. Therefore, DCH reserves the right to retrieve and read any data composed, transmitted or received through on-line connections and stored on DCH property and to monitor Internet sites visited or attempted. Inappropriate Internet or e-mail usage can expose DCH to significant legal liability and reflect discredit on the department.

B. DCH has installed software to prevent access to objectionable Internet and to monitor Internet access. The Division of Information Systems will periodically review and document Internet activity. Employees should be aware that any information accessed, downloaded, or transmitted may be reviewed by Systems staff and DCH management will be notified if an employee is repeatedly attempting to reach blocked sites or is frequently visiting non-work related sites.

C. When using DCH computers and resources to send or receive e-mail or to access Internet sites, employees are consenting to the monitoring of their use and have no reasonable expectation of privacy in the use of these resources.

D. DCH monitoring is limited and is done in an ethical and professional manner.

E. Failure to comply with this policy may result in disciplinary action, up to and including termination from employment.

Approved by:	Date: 10/22/08

Appendix A
Information Technology User Agreement

IT User understands that she or he will be given access to various DCH IT resources. IT User understands that he / she is responsible for helping to ensure the privacy, security, confidentiality and integrity of DCH IT resources over which he or she has control or to which he or she may have access. IT User will read, understand, and comply with the requirements below before accessing any DCH IT Resources:

I. Use of State Resources

- DCH IT resources, including but not limited to its e-mail and Internet services, information products and services, and computer hardware and software, are generally limited to official DCH business.
- IT User may not attempt to circumvent IT privacy or security safeguards, and any such attempts may lead to revocation of an IT User's access and may result in disciplinary action, as appropriate.
- 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 DCH policies, the Chief Information Officer (CIO) or his designee and the Director of Compliance 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.
- IT User may not add any network infrastructure. Network infrastructure additions may be done only by staff of the ITIS Section. Such network infrastructure includes, but is not limited to, routers, flash drives and wireless devices.
- IT User's supervisor will inform the IT Division when a user no longer requires access to IT resources.
- IT User will not relocate workstations, printers, scanners, etc., without proper authorization or assistance from the appropriate IT support staff.
- IT User will only physically connect to the DCH internal network using State of Georgia assets.
- IT User understands that if he or she brings any personal devices with electronic storage onto DCH premises, such devices are subject to monitoring and seizure if there is reason to suspect inappropriate use. At no point will IT User connect such devices to a DCH asset or to the internal network, unless approved by the DCH IT Division.
- IT User understands that he or she must comply with all DCH policies with respect to electronic communications.
- When accessing the Internet:

Information Technology User Agreement (Cont'd)

IT Users will not disclose confidential or protected health information in unencrypted e-mail and will use best efforts to send only e-mail content that is appropriate for transmission in that media, including e-mail messages that are professional, accurate, and factual. Users will be mindful of the right of any person to inspect and copy e-mails upon request, under the Georgia public records law.

II. Protection of State Resources

- IT User will safeguard passwords and other authentication devices, such as user I.D.s, and will not share them with anyone.
- IT User will encrypt any and all protected health information or other individually identifiable health information prior to transmitting it electronically.
- IT User will take reasonable steps to protect DCH resources from loss, damage, or theft and will understand that failure to do so may result in disciplinary action, as appropriate. Protecting DCH resources includes password protecting and safeguarding DCH laptops, PDAs (BlackBerry devices, etc.), and any personal computers or portable drives to which confidential or protected health information is transmitted or upon which it is stored. IT User will protect her or his assigned workstation from unauthorized access.
- IT User will not attempt to introduce malicious software or coding into DCH networks.
- IT User will not attempt to bypass, strain, or test security mechanisms, unless authorized as required by specific job responsibilities.
- IT User will not download any personal software, programs or files from the Internet onto a DCH computer. Any exception must be approved in writing by the Division of Information Services.

III. Licenses and Other Issues Related to Intellectual Property

If an IT User requires any computer software, equipment, or media that is not originally issued, he or she will complete a Purchase Request and forward the request to the DCH Help Desk in order that the proper licensing and agreements are obtained by the IT Division. Additionally, an IT User will not download, use or connect any unauthorized software, freeware, adware, shareware, media files or hardware onto any DCH network, workstation, PDA or other system, nor will he or she violate software copyright, trademark or license restrictions.

IV. Sanctions for Violations

Violations of this Information Technology User Agreement or the DCH Policy 419 will subject the employee responsible for the violation to disciplinary action, up to and including termination.