

 <p>GEORGIA DEPARTMENT OF COMMUNITY HEALTH</p>	<p>Policy Number: 910</p> <p>Effective Date: April 14, 2003</p> <p>Revision Date:</p>
<p>Privacy Policy</p>	<p>Safeguards</p>
<p>Originating Department: Privacy Office</p>	<p>Category: Legal Compliance</p>

SCOPE:

This policy applies to all Department of Community Health (DCH) employees, agents and contractors that perform duties in conjunction with the access, distribution, dissemination, modification, and management of protected health information.

POLICY:

It is DCH's policy to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule by establishing safeguard standards, and access controls for Protected Health Information that the Department collects and maintains. The intent of this policy is to establish criteria for safeguarding confidential information and to minimize the risk of unauthorized access, use or disclosure.

DCH will take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral and visual representations of confidential information.

Safeguarding confidential information – DCH workplace practices

Paper Records and Files

- Each DCH workplace will store files and documents in locked rooms or storage systems, where available. Where lockable storage is not available, DCH staff must take reasonable efforts to ensure the safeguarding of confidential information.
- Each DCH workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.
- Each DCH workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

Safeguards Policy – Page 2

Oral Information and Communications

- DCH staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
- Each DCH workplace shall make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.
- **Exception:** In work environments structured with few offices or closed rooms, such as in the cubicle workstations at 2 Peachtree Street, Atlanta, or other open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that DCH has met the reasonable safeguards and minimum necessary requirements.
- Each DCH workplace must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

Visual Access to Confidential Information

- DCH staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
 - A. Computer screens: Each DCH workplace must make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
 - B. Paper documents: DCH staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

Safeguarding confidential information – DCH administrative safeguards

a. Implementation of role-based access and the Minimum Necessary Policy will promote administrative safeguards. Role Based Access is a form of security allowing access to data based on job function in accordance with DCH security procedures. Employees shall be assigned to an access group that will give members access only to the minimum necessary information to fulfill their job functions.

b. Conducting internal compliance reviews periodically will permit DCH to evaluate the effectiveness of safeguards. The DCH Privacy Officer will implement periodic reviews in order to evaluate and improve the effectiveness of current safeguards.

c. Development and implementation of department-wide security policies will enhance administrative safeguards. DCH staff will be required sign a document that constitutes a formal commitment to adhere to the department-wide security policies.

REPORTING VIOLATIONS:

Violation of this or any other DCH Privacy Policy is to be reported to the DCH Privacy Officer.

LEGAL AUTHORITY:

45 CFR §164.530(c) Administrative requirements. Standard: safeguards – determine access control levels

45 CFR §164.502(a)(1)(iii) Permitted uses and disclosures

Preamble to the Final Privacy Rule, pg. 82561 – 82562

Preamble to the Modifications to the Privacy Rule, pg. 53193 – 53195

SANCTIONS:

DCH will apply appropriate sanctions against members of its workforce who fail to comply with the DCH privacy policies and procedures or with the requirements of the regulations. Sanctions taken by HHS in enforcement against DCH are a separate matter.

Sanctions will be appropriate to the nature of the violation. For example, the type of sanction will vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern of improper use or disclosure of protected health information. Sanctions could range from warning to termination of employment with DCH.

Sanction policies will be documented so that employees are aware of what actions are prohibited and punishable. Training will be provided and expectations will be clear so individuals are not sanctioned for doing things that they did not know were inappropriate or wrong.

DCH will not impose sanctions for disclosures by whistleblowers or workforce member crime victims, where a disclosure is provided for by the privacy standards. In addition, complaints and cooperation in investigations under the privacy standards are not subject to sanctions.

For additional information, see the DCH Sanctions policy and procedures.

 <p>GEORGIA DEPARTMENT OF COMMUNITY HEALTH</p>	<p>Procedure Number: 910</p> <p>Effective Date: April 14, 2003</p> <p>Revision Date:</p>
<p>Privacy Procedures</p>	<p>Safeguards</p>
<p>Originating Department: Privacy Office</p>	<p>Category: Legal Compliance</p>

PURPOSE

DCH will implement appropriate physical, administrative and technical safeguards and access controls for confidential and protected health information the Department collects and maintains.

PROCEDURE:

I. Paper Records and Files

The risks of inappropriate access to paper documents require additional attention to how paper records are used and handled. DCH staff must take special care to ensure the protection and safeguarding of, and the minimum necessary access to, paper documents containing confidential information that are located on: Desks, Fax machines, Photocopy machines, Portable electronic devices (e.g., laptop computers, PDA's, etc.), Computer printers; and in common areas (e.g., break rooms, restrooms, elevators, etc.).

- Files and documents being maintained or stored:
 - A. Lockable desks, file rooms, open area storage systems must be locked.
 - B. Where DCH has desks, file rooms, or open area storage systems, that are not lockable, reasonable efforts to safeguard confidential information must be implemented.
- Files and documents awaiting disposal/destruction:
 - A. Office and cubicle containers: The DCH workplace will ensure that confidential information awaiting disposal is stored in containers that are appropriately labeled and are properly disposed of on a regular basis.

Safeguards – Procedures – Page 2

B. Centralized shredding bins: Each DCH workplace will ensure that all centralized bins or containers for disposed confidential information are clearly labeled “confidential” and sealed.

C. Each DCH workplace that does not have lockable storage rooms or Centralized shredding bins must implement reasonable procedures to minimize access to confidential information.

- Shredding of files and documents authorized consistent with record retention requirements:
 - A. DCH staff: Ensure that shredding is done timely, preferably on a daily basis.
 - B. Outside contractors: DCH will ensure that such entity is under a written contract that requires safeguarding of confidential information throughout the destruction process.

II. Oral Information and Communications

DCH staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs, and should be aware of risk levels.

- Locations of verbal exchange with various risk levels:
 - A. Low risk: interview rooms, enclosed offices and conference rooms.
 - B. Medium risk: employee only areas, telephone and individual cubicles.
 - C. High risk: public areas, elevators, reception areas and cubicles housing multiple staff where visitors are often present.

III. Visual Access to Confidential Information:

DCH staff will ensure that observable confidential information is adequately shielded from unauthorized disclosure.

- Computer screens: DCH offices must ensure that confidential information on computer screens is not visible to unauthorized persons.

Some of the means for ensuring this protection include:

- A. Use of polarized screens or other computer screen overlay devices that shield information on the screen from persons not the authorized user;
- B. Placement of computers out of the visual range of persons other than the authorized user;
- C. Clearing information from the screen when not actually being used;
- D. Locking-down computer work stations when not in use; and
- E. Relocating fax machines and network printers out of common traffic areas;
- F. Other effective means as available.

Safeguards – Procedures – Page 3

Administrative safeguards

- Role Based Access (RBA): Roles will be created and defined based on the information DCH uses, where it is located, how it is used and why. A determination of who should have access to the specific data will be established.

DCH managers and supervisors will decide the role of each of their staff and request exceptions based on the needs of their office. Managers are responsible for allowing access to enough information for their staff to do their jobs while holding to the minimum necessary standard.

- DCH managers and supervisors will:
Follow the instructions given in the training for DCH Managers and Supervisors to safeguard confidential information;

Foster a more secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving DCH goals.

Managers will update the safeguards as needed, seeking to achieve reasonable administrative, technical and physical safeguards.

Utilize the Security Policies to augment safeguard procedures.

REPORTING VIOLATIONS:

Violations of these procedures should be reported to the DCH Privacy Officer.

SANCTIONS:

DCH will apply appropriate sanctions against members of its workforce who fail to comply with the DCH privacy policies and procedures or with the requirements of the regulations. Sanctions taken by HHS in enforcement against DCH are a separate matter.

Sanctions will be appropriate to the nature of the violation. For example, the type of sanction will vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern of improper use or disclosure of protected health information. Sanctions could range from warning to termination of employment with DCH.

Sanction policies will be documented so that employees are aware of what actions are prohibited and punishable. Training will be provided and expectations will be clear so individuals are not sanctioned for doing things that they did not know were inappropriate or wrong.

Safeguards – Procedures – Page 4

DCH will not impose sanctions for disclosures by whistleblowers or workforce member crime victims, where a disclosure is provided for by the privacy standards. In addition, complaints and cooperation in investigations under the privacy standards are not subject to sanctions.

For additional information, see the DCH Sanctions policy and procedures.