2011 – HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT OF 1996

POLICY STATEMENT	DFCS is required to comply with the Health Information Portability and Accountability Act (HIPAA) of 1996, including its rules regarding security and privacy of confidential health information.
BASIC CONSIDERATIONS	HIPAA was enacted by Congress to provide group and individual insurance reform, introduce tax-related health care provisions, control healthcare fraud and abuse, and to ensure improvement in healthcare systems.
Covered Entity Status	The Georgia Department of Human Resources (DHR) has chosen Covered Entity status to promote simplification of information sharing within the Department.
Who Must Comply	This policy applies to all individuals who are Georgia Department of Human Resources (DHR) employees, volunteers, trainees, and contractors who perform duties in conjunction with the access, distribution, dissemination, modification, and management of protected health information.
Other Related Confidentiality Requirements	DHR administers programs and provides services that have more stringent requirements than those provided by the Privacy Rule. In the administration of such programs and provision of such services, the Department will adhere to the more stringent requirements.
PRIVACY RULE	The Privacy Rule, effective April 14, 2003, ensures privacy protection by limiting the ways that Protected Health Information (PHI) can be used and released.
Notice of Privacy Practices	**Each** adult AU/BG member and, if applicable, each PR must be provided with a Notice of Privacy Practices upon receipt of an application for assistance, or when he/she is added to an existing AU/BG. This includes instances in which an a/r is currently receiving benefits in another program, such as food stamps, and applies for Medicaid. The notice **must** be mailed to each adult who is not present for a face-to-face interview. It is preferable, but not required, that each adult sign and return his/her notice, however the case record must be documented that the notice(s) was sent.

PRIVACY RULE (cont.)

Personally Identifiable Information

PHI is individually identifiable health information. Examples of PHI include, but are not limited to the following:

- demographic information, such as name, age, gender
- health status information
- prescription drug information
- healthcare payment information
- prior existing conditions
- eligibility information
- authorization and referral certifications

PHI may be in electronic, paper-based, or oral form.

Minimum Necessary

Covered entities may use and share only the minimum amount of protected information necessary to accomplish a particular purpose.

DHR is responsible for determining the amount of PHI required per function. Upon determination of minimum necessary PHI, DHR will communicate this decision to all affected parties.

Use and Disclosure

The Privacy Rule prohibits the use and disclosure of PHI for purposes not related to treatment, payment, or health care operations.

The identity of a person requesting PHI and his/her authority to receive such information must be verified prior to release of PHI.

As a covered entity, DHR is permitted, but not required, to use and disclose PHI, without an individual's authorization in certain situations and for specific purposes.

The following uses and disclosures do **not** require authorization from the individual:

- treatment, payment, and health care operations (TPO)
- public health agencies activities
- health oversight and regulatory agency activities
- judicial proceedings and law enforcement investigations
- healthcare fraud investigations
- emergency situations
- de-identified information (health information not connected with information identifying the individual)

PRIVACY RULE

Use and Disclosure (cont.)

The following uses and disclosures **do** require authorization from the individual:

- third party disclosures
- marketing and fund raising activities
- non-health related affiliates
- underwriting or risk rating activities
- employment determinations
- sale, rental or barter of PHI
- psychotherapy records other than psychotherapy notes

Form 5459

Prior to the release of PHI that requires authorization, the A/R must complete and sign DHR Form 5459 (rev. 04/11/03), Authorization for Release of Information.

Signed, blank Forms 5459 are **not** permissible and may not be obtained or used for any purpose. Form 5459 may be used to release or obtain information **only** if the A/R or PR has specified on the Form 5459 to whom information is to be released or from whom information is to be obtained. At the point the A/R signs Form 5459 it must be dated. Form 5459 should be used within 30 days from the date it is signed.

Administrative Requirements

DHR will maintain compliance with HIPAA Privacy Rule administrative requirements including, but not limited to:

- designation of a privacy officer who is responsible for the development, implementation and maintenance of privacy policies and procedures
- development, implementation, and documentation of timely and effective privacy training.
- development, maintenance, and enforcement of complaint procedures
- enforcement of appropriate sanctions for failure to comply with HIPAA regulations

SECURITY RULE

The HIPAA Security Rule ensures the security of PHI by specifying how PHI is stored, transmitted, and accessed.

PHI Safeguarding Practices

Guidelines for safeguarding PHI include, but not limited to:

- PHI will be discussed with the A/R or PR only in private areas
- PHI will be discussed with staff members on a need-to-know basis and in non-public areas only
- telephone calls regarding PHI will be held in areas in which the conversation cannot be overheard
- computer monitors will be positioned in a way that does not permit observation by anyone other than the A/R or PR
- computer passwords will not be shared and will be recorded only in secure locations
- PHI will be disclosed only by those staff members authorized to do so
- access to fax machines will be limited to authorized staff
- case records, mail, documentation, and other materials containing PHI will be maintained in locked or otherwise secure locations, away from the general public
- staff members will wear appropriate agency-issued identification at all times
- PHI will be discarded in appropriate secure containers.

Administrative Requirements

DHR will maintain compliance with HIPAA Security Rule administrative requirements including, but not limited to:

- development and enforcement of information access control
- completion of internal security audits
- enforcement of physical safeguards including workstation/office guidelines
- enforcement of appropriate sanctions for failure to comply with HIPAA regulations
- development, implementation, and documentation of security awareness training.

BUSINESS ASSOCIATE AGREEMENT

HIPAA requires that covered entities notify business associates and contractors of their status as a covered entity and the requirement to adopt and implement standards and procedures for handling PHI. Additionally, business associates must be notified that they must comply with applicable provisions of the Privacy Rule.

A Business Associate is defined as any provider performing a function or providing a service involving use or disclosure of PHI, on behalf of the Department. The arrangement may be through formal or informal arrangements.

TRAINING

Appointing authorities must ensure and document that all DFCS employees complete HIPAA training as part of new employee orientation.

PENALTIES FOR NONCOMPLIANCE

HIPAA provides for both civil and criminal penalties for covered entities that misuse PHI.

For **civil** violations of HIPAA standards, the Office of Civil Rights (OCR) may impose monetary penalties up to $100 per violation and up to $25,000 for multiple violations.

Criminal penalties range from $50,000 and one (1) year in prison for certain offenses, to $100,000 and five (5) years in prison for offenses committed under false pretenses, up to $250,000 and ten (10) years in prison for offenses committed with the intent of personal gain or malicious harm.

ADDITIONAL INFORMATION

Additional HIPAA information is available at www.hipaa.dhr.state.ga.us and www.hhs.gov/ocr/hipaa.