Information Protection Policy

Purpose: Provide assurances made by DHR to its employees and clients regarding the protection of certain types of information, such as individually identifiable health information (HIPAA).

The DHR Information Protection Policy is composed of three associated policy statements:

> The first statement, the DHR Information Protection Statement, declares what is expected of DHR in protecting information and information assets entrusted to the agency.
>
> The second statement, the DHR Employee Information Confidentiality Statement, is the DHR declaration for handling confidential employee information.
>
> The third statement, the DHR Client Information Confidentiality Statement, is the DHR declaration for handling client privacy information.

The DHR Information Protection Policy is a DHR Agency-wide Information Security Policy maintained and enforced by DHR. The penalties for a violation of these policies, including subordinate standards, practices and procedures may include criminal prosecutions, fines or other civil penalties, administrative sanctions, or any combination thereof.

Implementation and Maintenance: The DHR ISO is responsible for implementing all changes directed from the DHR Enterprise Security Steering Committee.

I. DHR Information Protection Statement

In order to protect DHR information from unauthorized disclosure, every DHR information user must exercise due diligence in protecting DHR information and the DHR information infrastructure. For this reason, every authorized user is responsible for protecting DHR property entrusted to their use, including all information assets.

Information assets include all information used, stored, or transiting in the DHR information infrastructure, as well as the supporting computer, network, and data center environments. An ***authorized information user*** is a person ***formally granted access to certain information and information assets*** based upon a ***job-related function and meeting need-to-know, right-to-know, and time–to-know criteria.*** An **unauthorized information user** is anyone **not having formally granted access** to information and information assets **or one that has not met the job-related function, need-to-know, right-to-know, or time-to-know criteria**. Unauthorized information users are subject to all provisions of the Computer Systems Protection Act — O.C.G.A., §§ 16-9-90 to 16-9-94, or other laws of the State of Georgia as appropriate.

Protection of DHR information assets includes the following:

1. DHR is responsible for ensuring employees, consultants, contractors, agents, suppliers and other state government organizations as appropriate formally accept their individual obligations and responsibilities to protect DHR information, assets and, resources.

2. DHR is responsible for ensuring access to DHR information assets and resources entrusted by DHR to third parties is authorized, controlled, and monitored based upon job-related function and need-to-know, right-to-know, and time–to-know criteria.

3. DHR is responsible for ensuring information owners and custodians protect DHR information assets and those entrusted to DHR by third-parties.

4. DHR is responsible for communicating to all employees, vendors, contractors, and others as appropriate this DHR Information Protection Policy. Furthermore, DHR is responsible for ensuring awareness of and adherence to DHR security standards, practices, and procedures where appropriate.

5. DHR is responsible for ensuring all DHR information, assets and the actions of DHR users, as well as information safeguards are in compliance with all applicable laws and regulatory requirements.

6. DHR is responsible for ensuring DHR information assets and resources entrusted to DHR by third parties are protected appropriately.

7. DHR is responsible for ensuring employees, consultants, business associates, service providers, agents, suppliers and other independent contractors are held accountable for safeguarding DHR information, assets, and resources and those entrusted to DHR by third parties.

8. DHR is responsible for ensuring employees, consultants, business associates, service providers, agents, suppliers and other independent contractors are held accountable for maintaining the confidentiality and integrity of the personal information held about employees and clients.

9. DHR is responsible for maintaining business continuity and supporting contingency plans for information, assets, resources, and business processes.

10. DHR is responsible for reporting and responding to all known and/or suspected breaches of DHR policies, standards, practices, and procedures.

11. DHR is responsible for compliance with the Employee and Client Information Confidentiality Statements that follow.

II. Employee Information Confidentiality Statement

In order to protect DHR employee confidential information from unauthorized disclosure, every DHR information user must exercise due diligence in protecting the DHR information infrastructure. For this reason, every user, whether employee, consultant, agent, or business associate is personally responsible for protecting DHR property entrusted to their use, including all information assets. Information assets include the computing environment, processes, systems, applications, databases, and all information stored or transiting through the DHR infrastructure.

Handling of DHR employee confidential information includes the following:

1. DHR collects, uses, and retains only relevant and necessary employee information.
2. DHR tells DHR employees what personal information DHR collects and how the information may be used to conduct legitimate business.
3. DHR strives to ensure the accuracy of employee information.
4. DHR tells DHR employees how they can review and correct information DHR maintains about them.
5. DHR appropriately restricts access to employee information.
6. DHR uses appropriate information security safeguards.
7. DHR uses general monitoring of employee activities to the extent necessary to protect DHR assets in accordance with applicable law.
8. DHR limits disclosure of employee information to external parties.

III. Client Information Confidentiality Statement

DHR's goal is to provide quality services that anticipate and fulfill client needs for service, confidentiality, integrity and availability. This Client Information Confidentiality Statement is intended to provide DHR employees with an understanding of the importance DHR places on maintaining the confidentiality and integrity of personal information in the delivery of DHR client services.

In order to protect DHR client confidential information from unauthorized disclosure, every DHR information user must exercise due diligence in protecting the DHR information infrastructure. The DHR Information infrastructure includes the computing environment, processes, systems, applications, databases, and all information stored or transiting through the DHR infrastructure.

Handling of DHR client confidential information includes the following:

1. DHR recognizes the obligation to keep information about DHR clients secure and confidential.

2. DHR complies with all applicable laws and regulations relating to the protection and security of client information.

3. DHR collects only client information necessary to conduct DHR activities.

4. For HIPAA purposes DHR must tell clients how their information will be used and disclosed.

5. DHR strives to ensure the accuracy of client information.

6. DHR extends this Client Information Confidentiality Statement to its business associates. DHR requires business associates, suppliers, vendors, and other state agencies to comply with DHR Information Security Policy fully.

7. DHR holds its information users responsible and accountable for this Client Information Confidentiality Statement.

Information Users Policy

Purpose: This policy provides notice to DHR information users regarding the scope of activities authorized, acceptable use of granted access and use of information obtained.

In order to protect certain DHR information from unauthorized disclosure, every authorized DHR information user must exercise due diligence in protecting the DHR information infrastructure. For this reason, every authorized user is responsible for protecting all DHR information assets.

Information assets include all information used, stored, or transiting in the DHR information infrastructure, as well as the supporting computer, network, and data center environments. An ***authorized information user*** is a person ***formally granted access to certain information and information assets*** based upon a ***job-related function and meeting need-to-know, right-to-know, and time-to-know criteria***. An **unauthorized information user** is anyone **not having formally granted access** to information and information assets **or one that has not met the job-related function, need-to-know, right-to-know, or time-to-know criteria**. Unauthorized information users are subject to all provisions of the Computer Systems Protection Act — O.C.G.A., §§ 16-9-90 to 16-9-94, or other laws of the State of Georgia as appropriate.

1. Users of DHR information assets shall have no expectation of privacy and DHR reserves the right to monitor information use and information system activity in accordance with applicable laws of the State of Georgia.

2. The DHR declares that all information collected, gathered, reported to or used by DHR in furtherance of DHR activities is an asset of DHR.

    a. Information assets are further defined as any data gathered, communicated, used, or observed by any information user in the course of their employment or relationship with DHR.

    b. Information includes, but is not limited to: technical, employment, vendor, health, locator, financial, or other information similar to the foregoing not specifically identified as public information. This data may exist in any form, including paper, voice, or electronic.

3. Information assets are to be protected by all individuals gaining access and should be used only in furtherance of authorized DHR activity. Such assets are necessary in order for DHR to remain capable of rendering the services required. Failure to protect information assets may cause irreparable damage to DHR, violate regulatory requirements, and erode public confidence in the DHR mission.

4. Access rights to DHR information are granted on a limited basis only and for the explicit purpose of conducting authorized DHR business. In order for an access right to be granted, each user must be considered for access based on an individual need-to-know, right-to-know, and time-to-know basis.

    a. If DHR has not granted access rights to a specific user for a specific purpose, the user is unauthorized.

    b. DHR access rights are allowed for no purpose other than those for which the access right was given.

    c. Users must request modifications to their access rights as the business needs change, no change of access rights may be assumed as being automatically granted and based on position of authority or expectation.

    d. User ID and Password control the rights to access DHR information. Disclosure of passwords may be unlawful under O.C.G.A § 16-9-93, which prohibits disclosing a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is unauthorized. If such a disclosure damages the computer or computer network, a fine of up to $5,000.00 and incarceration for a period of up to one year may be imposed upon conviction of computer password disclosure.

5. At no time are DHR information users permitted to share regulated or privacy based information with anyone except as specifically authorized by law.

6. All DHR information users must take proactive steps to prevent inadvertent disclosures of sensitive information or access to information assets. The intent of this action is to preclude disclosure from computer screens left unattended, unobstructed views of computer screens, or paper documents left exposed thereby allowing others without a need-to-know or right-to-know to gain or attempt to gain access to the information or information assets.

7. Specific requirements for protecting DHR information and information assets are further defined by DHR Information Security Standards. As DHR Information Security Standards, Practices, and Procedures will change from time to time it is the responsibility of Department to inform employees of changes and expect employees to conform.

8. DHR information users are not permitted to copy, sell, or re-issue any DHR owned software. Such violations will be a clear violation of the Information Users Policy and may be subject the user to civil, criminal, or administrative sanctions or any combination thereof as appropriate.

9. DHR information users are not permitted to load or use any individually purchased software, shareware, freeware, or other computer programs, including screen savers, on any DHR owned computer or information systems network without explicit written permission of the DHR ISO or a designated representative. Such violations will be a

clear violation of the Information Users Policy and may be subject the user to civil, criminal, or administrative sanctions or any combination thereof as appropriate.

10. Exceptions to this policy must be communicated to the DHR Information Security Officer immediately. Requests for exceptions to any provision of this policy post-incident will be not be considered and will therefore constitute a clear violation of this policy.

11. Known policy violations must be reported to the DHR Information Security Officer immediately.

12. The DHR Information Users Policy is a DHR Agency-wide Information Security Policy maintained and enforced by DHR. The penalties for a violation of this policy may include criminal prosecutions, fines or other civil penalties, administrative sanctions, or any combination thereof.

I have read, understand, and agree to be bound by this Georgia Department of Human Resources Information Users Policy.

Beverly J. Walker
Print

Bev J Walker
First Name Middle Initial Last Name Signature

4/20/05
Date (MM/DD/YYYY)

Print

Witness First Name Middle Initial Last Name Signature