Georgia Department of Community Health	**Policy and Procedure**		
Title:	Managing Authorization, Access, and Control to Information Systems and Request for Network Access Form		
Policy #:	435	Pages: 14	
Document Type:			
Effective Date:	August 16, 2012	Implementation Date	February 1, 2013
POC for Changes:	Chief Operating Officer		
References:	(1) Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, Privacy Rule and Security Rule. (2) Georgia Technology Authority (GTA) Enterprise Security Policy Authorization and Access Management (GTA PSG: SS-08-010.01) (3) Appropriate Use and Monitoring (GTA PSG: SS-08-001.01) (4) Federal Information Security Management Act (FISMA) Reference 4: Security Planning (5) FISMA References 4-Security Planning, 5-Personnel Security, 12-Awareness and Training, 15-Access Control, 17-Audit and Accountability (6) Policy 419: DCH IT-Use of State Computers and the Internet (7) DCH Enterprise Security Policy		

I. Purpose

A. Provide the general framework of the policy and procedure utilized by the Department of Community Health (DCH) to control access to information and associated applications governing agency operations;

B. Clearly document information access control policy and procedures;

C. Avoid the negative consequences that result when information systems are compromised, which consequences may include:

1. Sanctions;
2. Negative media attention;
3. Exposure of personal or private information and subsequent harm to individuals; and
4. Unauthorized access to DCH's applications including unauthorized viewing, modifications, and copying of data.

D. Provide for the development of access controls required to protect state and federal information systems.

E. Mitigate the risk of threats or incidents involving current or former employees or contractors who intentionally exceed or misuse an authorized level of access to a network or system or access data in a manner that affects the security of DCH data, systems or daily business operations.

F. Outline managers' responsibilities and role in managing authorization, access to and control of DCH's systems and applications as outlined specifically and agreed to in DCH Information Technology User Agreement.

G. Establish access control requirements for DCH contractors and business owners, as well as vendors, sponsors, and partners, in regards to their role and responsibilities, when access to DCH data and/or use of applications associated with DCH operations is authorized.

1. Reinforce the role of the business owner in providing adequate oversight of contractors' responsibilities specific to access control outlined in DCH contracts.
2. Ensure that valid business needs for access associated with DCH assignments continue to exist and that those needs are periodically reviewed and evaluated.
3. Assure compliance with all laws that require access controls procedures, including those identified as "References" in the header at the beginning of this document.

II. Policy

A. DCH information shall be used solely for appropriate agency purposes so that reasonable efforts are made to prevent any use or disclosure of Protected Health Information (PHI) in violation of HIPAA.

1. DCH information shall not be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with his or her role as stated in Policy **419**: DCH IT Use of State Computers
2. Those authorized to grant or revoke access to DCH information are responsible for following applicable procedures to ensure that access is appropriately assigned, modified as needed, and canceled promptly when individuals transfer to other positions or leave DCH.
3. Those accepting confidential information on behalf of DCH shall ensure that the requirements related to the acceptance of that information are followed.
4. Addressing the misuse of Department information and violations of IT Policy 419 is of paramount importance to DCH and will be dealt with on a priority basis. Alleged violations of this policy will be investigated in accordance with the appropriate legal requirements and DCH disciplinary procedures, and when appropriate, sanctions, including, but not limited to, dismissal, will be imposed.

B. Unless specifically designated as a public information system, access to any DCH information system network and its resources shall require the use of identification and authentication credentials in accordance with Policy 419 and the terms of applicable contracts.

C. All **contracts** that involve access to DCH systems shall include the requirement that DCH's IT Division be notified (in accordance with DCH instructions) immediately (and, in no event, more than 1 business day) after any modification or termination of roles. This applies to all DCH business owners, contractors, and vendors.

D. Access authorization shall follow the guidelines established by this policy and procedure.

E. Access authorization shall be documented, monitored and managed in accordance with state and DCH guidelines.

F. DCH deploys Role Based Access control measures which are based on an individual's role and responsibilities with DCH.

G. Roles are assigned by the Supervisor/Manager based on an employee's function within the organization.

H. Supervisors/Managers are responsible for validating and communicating roles and access, where the level of access to be authorized is the lowest level required for users to meet their DCH responsibilities.

I. Upon termination of employment or reassignment of job responsibilities, an employee's user id's and password shall be deleted in accordance with the DCH Enterprise Security policy.

J. Upon re-assignment of job responsibilities, an employee's access privileges shall be changed accordingly.

III. Scope

A. This policy establishes requirements for individuals regarding access to all DCH information, including the responsibilities of stewardship and accountability for DCH information needed in carrying out DCH's mission and/or conducting DCH business.

B. This policy refers to information systems that are used by DCH. Access control is required in order to comply with federal and state regulations and to safeguard the confidentiality, integrity and availability of sensitive and confidential information, including PHI.

C. This policy describes those procedures necessary for requesting, modifying and deleting user access to systems, applications and data covered by federal, state and all other applicable rules and regulations.

D. This policy applies to all who have access to DCH systems but whose access is not specified in a Business Associate Agreement or a Data Use Agreement.

IV. Roles and Responsibilities

A. Georgia Technology Authority (GTA): GTA manages access to the State's technology infrastructure and network services. GTA also controls some applications used by DCH. In addition, GTA manages administrative and physical access to systems. GTA is responsible for all matters related to the State's contracting with outside parties for GETS functions.

B. Georgia Building Authority (GBA) manages the office space occupied by DCH and provides the physical security necessary to provide a secure environment for people, equipment and information. GBA also manages the Building Access Request System, and physical access to the building.

C. DCH Offices, Management, and Staff

1. Commissioner

   a) Leads DCH and conveys the importance of information security to DCH management and staff.

   b) Supervises the CIO and communicates with other State leaders and the Governor's Office to promote efficient and effective information security measures.   The Commissioner has the final authority regarding the granting or termination of information access rights.

2. Chief Information Officer (CIO)

   a) Designates a senior agency information security officer (SAISO) who shall carry out the CIO's responsibilities for information security access control planning and implementation.

   b) Provides guidance and oversight regarding all DCH information security policies, procedures, and access control safeguards to address identity and access management.

   c) Oversees the identification, implementation, and assessment of security access controls throughout DCH's Technology Enterprise.

   d) Ensures that personnel with responsibilities for system, network, and application security access controls are appropriately trained.

   e) Assists other senior DCH management with their responsibilities for system, network, and application access security.

   f) Oversees the coordination of cross-platform security access controls for DCH.

   g) Collaborates with the Executive Director of GTA and other State CIO's to address technology and security issues, policies, and standards.

3. Information Security Officer [in the Office of Information Technology (OIT)]

   a) Manages information security access control planning and implementation on behalf of the CIO.

b) Coordinates the development, review, and acceptance of security access controls with IT system owners, access security administration staff, and business owners or authorizing officials.

c) Coordinates the identification, implementation, and assessment of network, system, and application access security controls.

d) Plays an active role in developing and updating security access control policies, procedures, and standards and assesses the security impact.

e) Collaborates with the State Chief Information Security Officer and other State agency Information Security Officers to address Enterprise Security Access Control Policies, Procedures, and Standards and their impact on DCH business operations.

f) Provides oversight and guidance to security administration and operations staff regarding security access control policies, procedures, and standards.

4. Access Control Coordinator/Systems Administrator

a) Sets and administers system-wide security controls appropriate for the authority given to users in accordance with the attributes or privileges associated with access control systems.

b) Acts as the first step of security by creating user id’s and passwords to access the local file servers.

c) Is appointed by CIO as the owner and manages the authorized access list.

d) Acts as the primary point of contact to control settings and coordinate administrative changes for statewide applications, including assigning permission for certain functions and access levels.

5. Inspector General

a) Oversees the criminal background check process for all DCH employees.

b) Coordinates with Director of Human Resources to ensure proper background checks for independent contractors and temporary staffing agency employees are complete before access to information systems is granted.

c) Directs investigations related to violations of DCH information security procedures, including access control procedures, and works with the HIPAA Privacy and Security Officer to recommend sanctions.

d) Coordinates with the Attorney General and law enforcement when any information security incidents involve criminal behavior.

6. Chief Financial Officer (CFO)

The CFO is the primary authority for access by DCH staff to the PeopleSoft Financial System and related data. The CFO must approve the level of access to the Financial Systems before user id’s and passwords are created.

7. Contracts Administration

   a) Is responsible for ensuring that all contracts with business entities that have access to DCH information systems, or that operate information systems on behalf of DCH, includes provisions requiring the maintenance and implementation of acceptable information security controls, including access controls.

   b) Ensures that such contracts incorporate access controls related to DCH information systems and provide penalties for failure to promptly inform DCH of a need for access changes.

8. HIPAA Privacy and Security Officer

   a) Works with the CIO, Information Security Officer and Commissioner to revise DCH security controls as needed and ensure proper documentation in DCH policies and procedures.

   b) Works with the CIO, Information Security Officer and Director of Communications to promote compliance with HIPAA security regulations and ensure that all DCH workforce members receive regular security awareness training, including training on access controls.

   c) Works with the Director of Contracts Administration to clarify roles and responsibilities regarding HIPAA security compliance by business associates and develop contract language to address access controls.

   d) Works with the Director of Support Services to promote physical access controls, including physical security of information systems through worksite audits and support of secure document storage/destruction practices.

   e) Works with the Inspector General to investigate violations of DCH information security procedures and recommends sanctions for such violations.

9. Office of Human Resources

   a) Is responsible for ensuring that DCH maintains documentation showing that all independent contractors and temporary staffing agency workers have been properly screened in accordance with policies and procedures for background checks.

   b) Maintains documentation that each member of the DCH workforce has access only to those information systems necessary to perform his/her work.

   c) Ensures that all new members of the DCH workforce receive HIPAA Privacy and Security training, which includes training on access restrictions, before receiving access to DCH information systems.

   d) Ensures that all new members of the DCH workforce sign an acknowledgment of the DCH information security procedures.

e) Maintains HIPAA training and acknowledgment forms for DCH employees, and ensures that such forms are provided to the HIPAA Privacy and Security Officer for all independent contractors and temporary staffing agency workers.

f) Ensures that all supervisors are aware of their responsibility to approve information system access only as needed and change the access whenever a staff member's access requirements change.

g) Ensures that the process for termination of employment includes termination of access to information systems.

10. Support Services

a) Coordinates with GBA and GTA to ensure that physical access to DCH workspace and information systems storage is properly limited through badge access and other controls.

b) Works with law enforcement to notify DCH staff members of threats to information system arising from break-ins and thefts.

c) Coordinates with DCH and other State leaders to ensure that business continuity plans are current and appropriate.

d) Supports security breach investigations.

11. Director of Vendor and Grantee Management

a) Monitors compliance by vendors with information security provisions in service level agreements, including provisions related to access controls.

b) Is responsible for including information security audits in the vendor management audit process.

12. Director of Procurement/Agency Procurement Officer (APO)

The Director of Procurement/APO is the primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff. The APO must approve the level of access to the TGM system before a user ID and password is created for the employee.

13. System Administrators

a) Are uniquely responsible for enabling users to manage a system or server.

b) When appropriate, authorize users to define or alter user id's, set security controls on a system or alter system components. These higher level privileges are restricted and controlled and may be extended to performing system support and maintenance activities if not assigned at the enterprise level.

c) Authorize and manage users' access to systems (as listed in the Request for Network Access Form) with privileges defined by job function and role within DCH.

d) Serve as the primary business owners for the application/platform system with authorization to perform job functions.

e) Validate privileges annually and report updates to DCH Access Control Coordinator, and perform requested changes to DCH premium networks after ensuring that proper authorization has been obtained.

f) Retain revalidation results, evidence of completion and supporting communications for at least 6 years per HIPPA requirements, and define and manage access control requirements, including authorization processes and user ID and password rules for managed applications and systems.

g) Maintain event/activity logs on all actions for each application under their control.

h) Are primarily responsible for access to all DCH data closets. Entry for any other staff is strictly prohibited unless an emergency (e.g., fire or water damage) dictates otherwise.

14. Individual Users

a) Defined as any user or network member that requires access to any network, system, or application that accesses, transmits, receives, or stores electronic information.

b) User id's for DCH applications shall not be shared and individual accountability for security of those id's must be maintained.

c) Authorized users are responsible for keeping all account authentication information in a secure place and not permitting any other person to use such accounts for any purpose.

d) Authorized users shall use all necessary precautions to safeguard confidentiality of associated passwords and shall change passwords when directed to comply with scheduled security reviews.

e) Authorized users shall notify the CIO immediately if their password is compromised and is shall not use a password belonging to someone else.

f) The user is accountable for all activity performed using applicable id's.

g) Authorized users acknowledge that when they are no longer employees of DCH, authorization to use the account will be terminated.

D. State of Georgia recognizes three (3) types of user accounts: Service Account, User Account and Privileged Account. [Service Accounts can be privileged, if technically required, but User Accounts may not. All User Accounts should have a named owner and follow the password policies of the State

1. Service Account – Service Accounts are used to allow system services or applications to connect to a system. These accounts are not intended for individuals to use interactively.

2. User Account – User Accounts are designed for use by general users with non-privileged system access.

3. Privileged Account – Privileged Accounts enable a user to manage a system or server. They may allow a user to define or alter user id's, set the security controls on the system or alter system components. Access to Privileged Accounts is not granted to the general user and should be restricted and controlled.

V. Procedure

A. Manager/Supervisor/Business Owner shall:

1. Complete a Request for Network Access form (see Attachment A) to identify an individual DCH user who requires access to the DCH computer system/application. This form is required for access request initiation, updates, and terminations.
2. Scan and send the completed form electronically to the DCH Access Coordinator. Print and sign in the Manager Approval section to indicate approval for the access requested.
3. Keep the form in a secure, on-site location (e.g., the user's personnel file held by the Manager/Supervisor), readily available upon request.
4. Review the assignment of computer systems annually for employees under his/her direct supervision to ensure that business need still exists for the specific application.
5. Review access as users change positions or work assignments (e.g., promotion, demotion, transfer, role change, extended leave or rehire) to ensure that access is maintained or revoked, as appropriate.

B. Access Coordinator/Agency System Administrator shall:

1. Grant access as specified on the Network Access form and notify the manager/supervisor/business owner when complete.

2. Forward requests for specific applications to the designated system administrator.

3. Modify or revoke access privileges when users are operating outside their work assignments.

4. Revoke access privileges during a user's extended leave or when deemed appropriate by the Human Resources Office.

5. Request appropriate modification or termination of access privileges to information assets and data systems in accordance with the following:

   a) When the user terminates employment with DCH or the need for access no longer exists, access shall be terminated.

   b) After 60- 90 days of no logon to information systems or applications, access shall be terminated.

c) When there is unauthorized or wrongful use or disclosure of information, access shall be terminated in accordance with DCH Enterprise Security Policy.

d) Upon completion of a project or contract work, access shall be terminated and the application administrator shall be notified. A Request for Network Access Form must be submitted before access can be reinstated.

C. Access to Functions

1. Users shall be granted access only to the extent necessary to perform their functions at DCH. Access can be restricted to specific functions within some applications. Whenever the software allows, access should be as specific and limited as feasible. Users should only have read or write access to the specific ePHI data required for performing their appropriate function. In most cases, access will fall into one of the following categories:

   a) Administrator/Super-User; or

   b) Regular or Normal User Accounts

2. The minimum access control requirement is a username and strong password. Every user at DCH must have a unique username. User names shall not be shared. For more information on this policy, see IT Policy 419.

   a) Role-based access may be employed where it improves specificity of access. Role-based access allows end-users to access information and resources based on their role within the organization. Role-based access can apply to job categories or to groups of people or individuals.

   b) The use of Anonymous accounts violates this policy and is strictly prohibited. The use of anonymous user accounts that are able to access internal agency IT resources, including, but not limited to, PHI, is strictly prohibited unless specifically authorized in writing by the CIO.

3. If approved by the DCH Information Security Officer and the HIPAA Privacy and Security Officer, DCH may create user accounts for an entity other than DCH that are, in turn, authorized to create, modify and terminate sub-accounts. The security privileges of the user accounts must be approved by the DCH ISO and the HIPAA Privacy and Security Officer. The entities for which the user accounts are created must enter into a written agreement with DCH that describes both the security privileges and the proper use of the accounts. Each such agreement shall set out in specificity the requirements the entity shall follow, which procedures shall be similar to those established by Policy 435, and to maintain at all times Network Access Control forms approved by DCH which are substantially similar to the one attached to this Policy 435. The agreement shall include penalties or other appropriate consequences, as permitted by law, for failure to promptly terminate access, and shall require the entities to file quarterly updates showing the current users and affirming that their continued use and level of access continue to be appropriate or should be modified.

D. Eligibility for Access

1. Employees whose job responsibilities require access to PHI may be authorized to access specific applications which provide access to PHI, if appropriate, with the written approval of the System Owner and the HIPAA Privacy and Security Officer.

2. Contractors/Temporary Staff providing support to specific DCH functions on a time-limited basis may be authorized access to specific applications for the duration of their assignments with the written approval of the System Owner.

3. Access shall only be granted to users whose status with DCH is current.

4. Whenever job responsibilities change, the supervisor shall review and determine the appropriate access and request the corresponding changes by using the Request for Network Access Form.

5. If an individual no longer requires access (e.g., upon termination of employment) all access shall be terminated immediately.

E. Access Determination

1. Determining the access to specific applications necessary for job functions and responsibilities requires determining which applications are required based on those functions and the corresponding data needed.

2. Every user should be granted the lowest level of access necessary to meet his/ her DCH job responsibilities. This practice is intended to limit the damage that could result from accidents or errors.

F. Monitoring and Oversight

1. The Information Security Officer shall conduct periodic reviews to validate the appropriateness of user accounts and access privileges.

2. Supervisors and System Administrators shall review access requirements annually.

3. Supervisors shall review user access at least twice per year, which reviews can be accomplished during an employee's midyear and annual performance reviews to ensure that each user's access is appropriate.

4. System administrators shall review all user access periodically as a critical function of his/her responsibility to ensure that all users are in current status.

5. All system users consent to such monitoring and accept responsibility to preserve the confidentiality, integrity, and availability of information accessed.

G. Training and Access

1. All DCH employees shall complete HIPAA security training during their new hire orientation and during refresher training as designated by the HIPAA Privacy and Security Officer.

2. Regularly scheduled system activity reviews shall be conducted by System Administrators to ensure that the level of access to the system is appropriate.

VI. Supporting Documentation

PeopleSoft 8.9 HCM Security	Upon approval application is faxed to State Accounting Office, 200 Piedmont Avenue, Suite 1602 West Tower, and Atlanta, GA 30334. Fax # 404-463-5089.
HRM Query Access Request	Upon approval application is faxed to HRMS Phoenix Security, 200 Piedmont Avenue, Suite 1602 West Tower, and Atlanta, GA 30334. Fax # 404-651-5113.
PeopleSoft FN Financial 9.0	Forms can be faxed to 404-463-5089 Attn: Security or mail forms to: State Accounting Office, 200 Piedmont Avenue, Suite 1602 West Tower, Atlanta, GA 30334, Attention: Security.

V. Glossary of Terms

Access Control Coordinator	The authority given to an individual by the assignment of attributes or privileges that are associated with access control systems and that are required for setting and administering system-wide security controls. Individual is designated by the Chief Operating Officer.
Administrator/Super-User	A special user account used for system administration. Depending on the operating system, the actual name of this account might be: root, administrator or supervisor.
Agency Procurement Officer (APO)	Primary authority for access to the PeopleSoft Team Georgia Marketplace (TGM) data by DCH staff.
Contractor	An organization or individual that contracts with the Department to supply needed service or skill set.
Georgia Building Authority (GBA)	The State Authority that manages the property occupied by State agencies and provides the physical security necessary to provide a secure environment for people, equipment and information.
Georgia Technology Authority (GTA)	The State Authority that establishes information security standards and requirements for the State of Georgia.
HIPAA	Health Insurance Portability and Accountability Act, a US law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.
IT Sabotage	Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems, or data with the intention of harming a

	specific individual, the agency, the agency's data, systems, and/or daily operations.
Privileged Account	Accounts that enable a user to manage a system or server.
Protected Health Information (PHI)	Protected health information is defined in 45 CFR 160.103, 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.
Resource Access Control Facility (RACF)	Designed to provide improved security and controls what users can do on the operating system.
Role Based Access (RBAC)	An approach to restricting system access to authorized users. The primary rule for RBAC is as follows: Role assignment and authorization: A user shall be granted system access based on his/her assigned and authorized active role in DCH.
Security Planning	Requires organizations to have security controls in place or planned for their information systems and the rules of behavior for individuals accessing the information systems.
Service Account	Used to allow system services or applications to connect to a platform resource.
Theft Of Information	Cases in which current or former employees or contractors intentionally exceed or misuse an authorized level of access to networks, systems or data with the intention of stealing or modifying confidential or proprietary information for the organization.
Third Parties	Parties who contract with the DCH that administer applications, on the agency's behalf, that are covered by HIPAA security regulations or that represent significant financial risk to the DCH.
User Account	Defined as general users with non-privileged system access.

VI. Version Control

1.0	Plan approved by Commissioner David Cook	August 17, 2012
1.1	Request for Network Access form updated to reflect recommendations from Pilot Team and gap assessment completed thereafter.	January 23, 2013

Approved By: **Commissioner**	**Date** 5/16/13

GEORGIA DEPARTMENT
OF COMMUNITY HEALTH

Request for Network Access

User Please Read First: The purpose of this form is to gather pertinent information in order to provide employees or contractors with access to the Department of Community Health's network applications. Once signed, this form will serve as an attestation that the Employee named below requires access to the specified applications including some which may contain sensitive and protected information. Managers must comply with DCH**Policy 435:** *Managing Authorization, Access and Control of Information Systems* when granting and changing user access. Forms will be retained by the DCH Access Control Coordinator and by the Authorizing manager.

Instructions: This form applies to DCH employees, contractors, and consultants on assignment at the Department of Community Health. The Hiring Manager or Business Owner (contracts) is responsible for completing the form, obtaining the required authorizations, and for submitting it to the OIT. The form must be completed in its entirety each time access permissions are issued, modified or deactivated. Users must have been assigned either a Employee ID, Data Agreement #, or a Contract # in order to be eligible for network access. Please complete the form on-line or print and scan and send to the DCH Access Control Coordinator, clewis@dch.ga.gov, helpdesk@dch.ga.gov with a copy to the authorizing manager before access will be granted.

Section 1 Administration

Date Form Completed									
Req Type	New Hire	Termination	Change	Performance Evaluation	New Contract	Amendment	Contract Termination	Service Request Date	Other
"x' if applicable									

DCH Employee Information				DCH Contractor/Consultant Information			
Employee Name		Employee ID		Contractor Name		Company Name	
Employee Email				Contractor Primary Email			
Employee Title				Contractor Title			
Role				Business Owner (BO)			
Supervisor's Name				BO Email			
Authorizing Manager				BO Division	Medical Assistance Plan		
Division Name	Medical As	Unit Assigned		BO Assigned Unit			

Section 2 Physical Access and Equipment

Location ID		Office#/Wkst #		Badge#		R or B	

Physical Access Special Permissions

Access Permission in Restricted DCH Areas	OIG (5th Fl)	Y	N	SHBP (35th Fl)	Y	N	Other	

Request for IT Equipment

New Order	Y/N	Issue Date	Ret. Date	Asset #	Existing Equipment		Asset#
Desk Top (Y/N)					Desk Top (Y/N)		
Lap Top (Y/N)					Lap Top (Y/N)		
Blackberry (Y/N)					Blackberry (Y/N)		

IT Department Only

Approved	Y or N
Date Created	
Date Reviewed	
Initials	
Additional Comments	

Note: New Users receive standard software package: MS Office, Adobe Acrobat Reader, CITRIX, WinZip, Virus Scan, Internet Explorer, and MS Outlook.

Section 3 Request for Access to DCH Applications

Permissions		Permissions		Permissions	
Please Select from Drop Down box	Applications	Please Select from Drop Down box	Applications	Please Select from Drop Down box	Applications
	Dataprobe	Admin Only	PeopleSoft		
	CATS		Human Capital Management		Witness Call Reporting
	CRAMS (Contract Reporting &Monitoring System)	Remote	Financial Services		Other DCH Applications
	DFCS SUCCESS		Team Georgia Marketplace		
	GBA Badge Access		SharePoint		
	ITRACE		Vendor Management		
	Kronos		Grant Administration		
	Laserfische		SABA (Learning Management)		
	MEMS (SHBP)		Unified Arts/Voice Mail *		
	MEUPS-Production		VPN (Virtual Private Network)		
	MEUPS-Non Production				
	G:Drive Restricted Folders				
	0:Drive Restricted Folders				
	Budget				
	HIPAA Privacy & Security				
	Medical Policy (Medicaid Only)				
	PEHB Accounting				
	Personnel				
	S: Drive (SHBP Only)				

Key Terms and Definitions

Application Software that processes data for the user.

Authorizing Manager-a Manager designated in writing by a Division Chief as authorized to grant access to DCH IT systems.

Contractor-An organization or individual that contracts with the Department to supply a needed service or skill set.

Permission-An operation is a set of permissions that you associate with system-level or API-level security procedures like WriteAttributes or ReadAttributes. You use operations as building blocks for tasks.

Role: A role is a set of permissions that a user must have to do a job. Well-designed roles should correspond to a job category or responsibility (for example, receptionist, hiring manager, or archivist) and be named accordingly. With Authorization Manager, you can add users to a role to authorize them for the job.

Employee's Signature **Date**

Authorizing Manager's Signature **Date**

Instructions on how to complete this form are included for reference purposes only. If you require additional assistance please notify the Network Access Coordinator. Please provide as much information as possible.

Last Reviewed1/24/2013