

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0518	REVISION: Original	PAGE 1 OF 3
SUBJECT: Access Authorization and Modification		EFFECTIVE DATE	Draft: 02/17/05
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

This policy directs each Bureau/Office in the Department of Health and Human Resources (DHHR) to establish access authorization and modification procedures to control user access to Information Technology (IT) resources, which contain sensitive data and/or electronic Protected Health Information (e-PHI).

2.0 SCOPE

This policy applies to bureau commissioners, program directors, the Information Security Officer (ISO), and data owners within the DHHR.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 Health Insurance Portability and Accountability Act (HIPAA) of 1996
- 3.2 DHHR HIPAA Policy Memorandum 0401 – *Authorization to Use or Disclose Protected Health Information*
- 3.3 DHHR HIPAA Policy Memorandum 0423 – *Sanctions for Violating Privacy and Security Policies and Procedures*
- 3.4 DHHR HIPAA Policy Memorandum 0442 – *Termination or Modification of Access to Protected Health Information: Electronic Systems*
- 3.5 Reference: Federal Register 45 CFR §164.308 (a) (4)
- 3.6 DHHR IT Policy – 0501 – *Use of Information Technology Resources*
Attachment A – *Employee Responsibility*
Attachment B – *Unacceptable Uses of IT Resources*
- 3.7 DHHR IT Policy – 0510 – *Electronic Message (E-mail) Guidelines and Requirements*
Attachment A – *Granting Approval to Access E-mail Communications of Others*
- 3.8 DHHR IT Policy – 0511 – *IT Network Security*

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0518	REVISION: Original	PAGE 2 OF 3
SUBJECT: Access Authorization and Modification		EFFECTIVE DATE Draft: 02/17/05	

3.9 DHHR IT Policy – 0512 – *IT Information Security*
Attachment A – *Roles and Responsibilities*

4.0 RESPONSIBILITY/REQUIREMENTS

4.1 Bureau/Office Responsibilities

4.1.1 Each Bureau/Office will establish written procedures for both granting and modifying employee access to specific IT resources containing sensitive data and/or e-PHI.

4.1.1.1 Procedures will be developed and documented to comply with state and federal regulatory laws and associated compliance deadlines.

4.1.1.2 Procedures will be documented by a designated individual within each Bureau/Office.

4.1.1.3 Procedures will be submitted to and retained by the ISO or a designee.

4.1.2 Each Bureau/Office will require awareness training specific to the IT system(s) for which the employee is granted access.

4.1.2.1 Training will include responsibilities and duties associated with access to and acceptable use of e-PHI or sensitive data.

4.2 Enforcement Authority

4.2.1 The ISO is the person designated by the Chief Technology Officer (CTO) to monitor and provide initial enforcement of the DHHR's information security program and IT policies.

4.2.2 The Information Security Liaisons (ISL's) are employees assigned by the commissioner with each Bureau and/or Office to assist the ISO in the protection of information resources.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0518	REVISION: Original	PAGE 3 OF 3
SUBJECT: Access Authorization and Modification		EFFECTIVE DATE Draft: 02/17/05	

4.2.3 The Office of the Inspector General (OIG) is the authority who investigates reported instances of Departmental employee misconduct.

4.3 Violations and Disciplinary Action(s)

4.3.1 All suspected violations of this policy will be reported to a supervisor in the chain of command above the employee.

4.3.2 The supervisor or designee will review the facts and, if it is suspected that a violation may have occurred, the matter will be referred to his/her Office Director or Bureau Commissioner for appropriate action.

4.3.3 As determined by the Office Director or Bureau Commissioner, instances of abuse or misconduct, depending on the circumstances, will be referred to either the ISO or the OIG for further investigation.

4.3.4 Employees or systems administrators or managers who willfully or knowingly violate or otherwise abuse the provisions of this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy 2104; or (2) criminal prosecution.

5.0 DEFINITIONS

5.1 Access – The ability to locate, gain entry to, and use a directory file or device on a computer system or network.

5.2 Electronic Protected Health Information (e-PHI) – Health information transmitted by or maintained in electronic media that can be used to identify an individual and was created, used, or disclosed in the course of providing health care services such as diagnosis or treatment. Examples include: names, phone numbers, medical record numbers, photos, etc.

5.3 Employee - Individuals employed on a temporary or permanent basis by the DHHR; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office to be subject to this OP.