

DOCUMENT: <b>Policy</b>	DOCUMENT NUMBER: IT-0516	REVISION: Original	PAGE 1 OF 3
SUBJECT: <b>Audit Controls and Review</b>		EFFECTIVE DATE: 02/17/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

## 1.0 PURPOSE

This policy defines the responsibility of each Bureau within the Department of Health and Human Resources (DHHR) to develop audit controls and review procedures to record and examine information systems activity when sensitive data or electronic protected health information (e-PHI) is contained or transferred by the system(s).

## 2.0 SCOPE

This policy applies to Bureau Commissioners, Office Directors, the DHHR Information Security Officer (ISO), and data owners.

## 3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 The Health Insurance Portability and Accountability Act (HIPAA) of 1996.
- 3.2 Department of Health and Human Services (DHHS) Reference: Federal Register 45 CFR § 164.312
- 3.3 HIPAA Policy 0400 – General Policy Use and Disclosure of PHI
- 3.4 HIPAA Policy 0423 – Sanctions for Violating Privacy and Security Policies and Procedures
- 3.5 DHHR Policy Memorandum 2104 – Progressive Discipline
- 3.6 DHHR Policy Memorandum 2108 – Employee Conduct
- 3.7 OMIS Operating Procedure (OP) – 25 – Audit Controls

## 4.0 RESPONSIBILITY/REQUIREMENTS

- 4.1 Each Bureau/Office will work with the Office of Management Information Services (OMIS) or the appropriate technical resource to develop an *Audit Controls and Review*

DOCUMENT: <b>Policy</b>	DOCUMENT NUMBER: <b>IT-0516</b>	REVISION: <b>Original</b>	PAGE <b>2</b> OF <b>3</b>
SUBJECT: <b>Audit Controls and Review</b>		EFFECTIVE DATE <b>02/17/05</b>	

procedure to record and examine information systems activity involving sensitive data or e-PHI.

4.1.1 Audit logs will be used to monitor, document, and manage system and application activity.

4.1.2 Audit data may be categorized to include the following:

4.1.2.1 System and application log-in reports;

4.1.2.2 Activity reports; and

4.1.2.3 Exception reports.

4.1.3 An audit review will be conducted by each Bureau/Office at intervals specified by the HIPAA Security Officer or designee.

4.1.3.1 A report of findings will be generated from audit log data.

4.1.3.2 Audit review results will be submitted to the ISO or designee.

## 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 Liaison's (ISL) are employees assigned by the commissioner with each Bureau and/or Office to assist the ISO in the protection of information resources.

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.

DOCUMENT: <b>Policy</b>	DOCUMENT NUMBER: <b>IT-0516</b>	REVISION: <b>Original</b>	PAGE <b>3</b> OF <b>3</b>
SUBJECT: <b>Audit Controls and Review</b>		EFFECTIVE DATE <b>02/17/05</b>	

- 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 to this policy may be subject to: (1) disciplinary action as outlined in DHHR Policy Memorandum 2104; or (2) criminal prosecution.

## 5.0 DEFINITIONS

- 5.1 Access – the ability to read, write, modify, or communicate data/information or otherwise use any system resource.
- 5.2 Audit Controls – The use of hardware, software, or procedures to record and examine system(s) activity.
- 5.3 Audit Log – Captures the computer user’s actions while logged on to a system and saves the information to a database table or formatted file.
- 5.4 Data owner – The person having primary responsibility for the creation and maintenance of the data content.
- 5.5 Electronic Protected Health Information (e-PHI) – Health information transmitted by or maintained in electronic media used to identify an individual, and is 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.)
- 5.6 Information Security Officer (ISO) – The person designated by the CTO to monitor and provide initial enforcement of DHHR’s information security program and IT policies.
- 5.7 Office of Management Information Services (OMIS) – This office reports directly to the DHHR Deputy Secretary for Administration and provides the leadership, innovation, and services needed to achieve efficient and effective technology solutions to meet the goals of the DHHR.