

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 1 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE: 04/15/05	
OFFICE OF MIS:		DATE:	
SECRETARY OF DHHR:		DATE:	

1.0 PURPOSE

The purpose of this policy is to ensure that Department of Health and Human Resources (DHHR) data and electronic Protected Health Information (e-PHI) are protected from improper alteration or destruction in a manner proportionate to the associated risk when it is transmitted from one point to another.

2.0 SCOPE

This policy applies to all DHHR employees whose work or system support involves the transmission of e-PHI or other sensitive data.

3.0 APPLICABLE DOCUMENTS/MATERIALS

- 3.1 In instances where state and federal laws and regulations are more restrictive than DHHR IT policies, the more restrictive provisions will supersede.
- 3.2 The Health Insurance Portability and Accountability Act ([HIPAA](#)) of 1996.
- 3.3 DHHR [HIPAA Policy 0423](#) – Sanctions for Violating Privacy and Security Policies and Procedures
- 3.4 DHHR [HIPAA Policy 0441](#) – Safeguards to Protect the Privacy of Protected Health Information
- 3.5 DHHR [HIPAA Policy 0449](#) – General Guidelines to Safeguard Protected Health Information
- 3.6 DHHR [IT Policy 0510](#) - E-Mail Guidelines and Requirements
- 3.7 Office of Management Information Services (OMIS) Operating Procedure (OP) -12 – E-Mail Guidelines
- 3.8 OMIS OP-18, Managing Information Security Incidents

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 2 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

3.9 DHHR Policy Memorandum [2104](#) – Progressive Discipline

3.10 DHHR Policy Memorandum [2108](#) – Employee Conduct

4.0 RESPONSIBILITIES/REQUIREMENTS

4.1 Transmission Outside the DHHR Network

4.1.1 All transmission of sensitive data or e-PHI outside of the DHHR network must utilize an OMIS-approved Virtual Private Network (VPN).

4.1.1.1 Dedicated system-to-system connections do not require mandatory encryption controls.

4.2 Transmission Using E-Mail

4.2.1 All messages, attachments, files, and folders transmitted within the DHHR e-mail system are automatically encrypted.

4.2.2 E-mail transmitted outside the DHHR network is not encrypted, and should not be sent if the message or its attachment contains e-PHI.

4.3 Transmission Using Wireless LANs and Devices

4.3.1 The transmission of sensitive data or e-PHI over a wireless network within the DHHR is permitted only when the following conditions are met:

4.3.1.1 The wireless network is using the OMIS-approved authentication method to ensure that wireless devices connecting to the network are authorized; and

4.3.1.2 The wireless network is utilizing the OMIS standard encryption mechanism for all transmissions.

4.4 OMIS Responsibilities

4.4.1 OMIS will prescribe a comprehensive internal security control program to protect e-PHI and other sensitive data from improper alteration or destruction, and keep it consistent with its source.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 3 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

4.4.2 OMIS will ensure that all systems containing e-PHI and other sensitive data are designed to maintain data integrity.

4.4.3 OMIS will conduct a risk analysis to ensure that e-PHI or sensitive data is reasonably protected from associated risks when transmitted from one point to another.

4.5 Data Owner Responsibilities

4.5.1 The data owner will review the results of a risk analysis to identify which data must be protected from improper alteration or destruction.

4.5.2 The data owner will coordinate with OMIS to ensure that all information containing e-PHI or sensitive data is protected from alteration during transmission.

4.5.3 The data owner(s) or designee(s) will keep a record of all e-PHI or sensitive data in each Bureau/Office.

4.6 Employee Responsibilities

4.6.1 Prior to transmission, employees must notify the data owner of any material containing e-PHI or sensitive data.

4.6.2 Employees are prohibited from using any DHHR system to store or transmit sensitive data or e-PHI that does not have adequate authorization mechanisms.

4.6.3 When transmitting e-PHI or sensitive data, regardless of the transmission system being used, employees must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the data requested.

4.7 Enforcement Authority

4.7.1 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.

4.7.2 The Information Security Liaisons (ISL) are employees assigned by the Bureau Commissioners and/or Office Directors to assist the ISO in the protection of information resources.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 4 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

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

4.8 Violations and Disciplinary Action(s)

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

4.8.2 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.

4.8.3 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.

4.8.4 Employees 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 DEFINITONS

5.1 Data owner – The person having primary responsibility for the creation and maintenance of the data content.

5.2 Electronic Protected Health Information (e-PHI) - Health information transmitted by or maintained in electronic media used to identify an individual, which 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.

5.3 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 policy. For the purpose of this policy, this also refers to anyone using a computer connected to the DHHR network.

5.4 Encryption – The process of enciphering or encoding data so that it is inaccessible to unauthorized users.

DOCUMENT: Policy	DOCUMENT NUMBER: IT-0519	REVISION: Original	PAGE 5 OF 5
SUBJECT: Data Transmission Security and Integrity		EFFECTIVE DATE 04/15/05	

- 5.5 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.
- 5.6 Integrity – The ability for an entity to protect data from improper alteration or destruction and to assure e-PHI in its possession is kept consistent with its source.
- 5.7 LAN – A communications network made up of servers, workstations, a network operating system, and a communications link that serves users within a confined geographical area.
- 5.8 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.
- 5.9 Virtual Private Network (VPN) - A way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.