



# University of Connecticut Health Center

**POLICY NUMBER 2003-31**

**April 14, 2003**

**POLICY: UCHC DATA CLASSIFICATION POLICY  
(Privacy & Security of Protected Health Information (PHI))**

**PURPOSE:**

A) To clearly articulate the principles for implementing information security classification and commensurate protections for all electronic information at the UCHC.

B) To establish a framework for the administration of the information security classification process.

**POLICY STATEMENT:**

An effective information security program is based on the theory that the costs to protect an information asset should not exceed its value to the corporation.

This policy presents the major security risks to electronic information at UCHC. These risks include but are not limited to unauthorized destruction, modification disclosure, access, use, and removal of UCHC data. Furthermore, a program for establishing the sensitivity or value of each information set and classifying the data based on the relative level of confidentiality will be outlined.

The level of confidentiality or classification for individual information set can be derived by systematically considering the impact to the institution should the information fall victim to any or all of the major security risks. Information created and/or owned by the University of CT Health Center (UCHC) is a valuable asset and will be protected from all known security risks.

**I. Policy Detail**

**A. Risks to Information**

The major risks to information assets are destruction, modification disclosure, access, use, and removal. To properly manage information assets all three major risks should be considered. Historically, only disclosure has been addressed by information security. This policy outlines steps to remedy this traditional shortcoming.

**B. Classification of Information Assets**

The categorizing of information assets permits the establishment of a framework that can identify for each set of electronic information:

- Level of confidentiality
- Protective measures
- Individuals responsible for ensuring a constructive and consistent security process is established.

## II. Classification and Protection Framework

### A. Establishing the Level of Confidentiality

Not all information is subjected to the all the major risks to the same degree. All data sets that contain Protected Health Information (PHI) are clearly the most sensitive and automatically receive the highest classification level (i.e. Registered Confidential). Other highly sensitive applications that produce income, control the financial worth of the UCHC or contain proprietary information should be compared against the criteria listed in figure one and designated with the appropriate classification.

Information shall be protected through cost effective means. Not all information is of equal value or equally subject to compromise. Therefore, not all information requires the same level of security. By establishing proper classification of information, the truly sensitive can receive the special attention and handling it requires without adding expensive controls over information sets when not justified.

The following data classifications and definitions shall be used:

#### 1. Classified:

Registered Confidential - Information, if exposed to any of the major security risks, that would violate federal HIPAA security or privacy regulations and violate federal or state law. Only a senior administrator of the UCHC may designate information sets as Registered Confidential or grant access to this data. All data sets that contain PHI automatically receive this classification level.

Confidential – Information that should be accessed only by a limited group of authorized people (e.g. payroll information, personnel records, Etc).

Internal Use Only Information intended to be generally releasable within the Health Center but not to the general public (e.g. strategic plans, financial performance data, Etc.)

#### 2. Unclassified

Public/Unclassified - Information obtained from the public domain or over which the Health Center wishes to exercise no proprietary rights or which has been released through official UCHC channels. All data not classified in one of the three categories above, falls into the unclassified designation by default. Unclassified data requires no protective measures and no personnel are asked to exercise any particular actions according to this policy in support of this type of data. Section C included below does not apply to unclassified data sets.

- B. Protective Measures  
See figure one for detailed protective measures for each classification level:

**Figure One – Protective Measures**

Types of Information	Classification Level	Potential Loss Impact	Accessible Via FOI	Required Protective Measures
<b>Medical Records</b> <b>Patient Health Information (PHI)</b> <b>Clinical Trial Data</b>	Registered Confidential	<b>High</b> 	No	<a href="#">a) Authentication</a> Two Factor Strong Passwords Individual Passwords <a href="#">b) Application/Host Based</a> Session Timeouts Session Screen Lockouts Physical Host/PC Security OS Security Updates Disabled Utilities TCP-IP Wrappers Secure Shell Scheduled Audits <a href="#">c) Network Based</a> Encryption for Remote/WiFi Behind Firewalls Intrusion Detection
<b>Unpublished:</b> <b>Strategic Plans</b> <b>Investment Strategy</b> <b>Trade Secrets</b> <b>Intellect Property</b>			Per Case Basis	<ul style="list-style-type: none"> <li>•Patient Confidentiality</li> <li>•Regulatory Violations</li> <li>•Other Legal Liability</li> <li>•Customer Confidence</li> <li>•Conflict of Interest</li> <li>•Competitive Advantage</li> <li>•Financial Exposure</li> <li>•Employee Privacy Violations</li> <li>•Disclosure of Intellectual Property</li> </ul>
<b>Financial Data (unpublished)</b> <b>Access Security Profiles</b> <b>HR Personnel Records</b> <b>Proprietary Software</b> <b>Electronic Research Data</b> <b>Intellectual Property</b>	Confidential		Yes	
<b>Org Charts</b> <b>Policies</b> <b>Curricula</b> <b>Employee Manuals</b>	Internal Use Only		Yes	None
<b>Everything Else e.g.</b> <b>Vendor Knowledgebase's</b> <b>Electronic References</b> <b>Equipment Manuals</b>	Public Unclassified	<b>Low</b>	Yes	None

C. Roles of Responsible Personnel for Classified Information Sets (Information Owner, Steward, Custodian and User)

The UCHC senior administration delegates the authority to manage owned electronic assets to the appropriate levels of management. These managers have a responsibility to directly provide or assign stewardship over these assets. Information Technology has the responsibility for providing appropriate tools enabling the stewards to monitor and enforce the required access controls and data protections. IT acts in a custodial role carrying out the instructions of the steward in accordance with approved policies, standards and procedures.

Those individuals who require access to information assets are referred to as users. Users must obtain authorization from the appropriate steward before attempting to access electronic data. The custodian shall provide for the technical means to prevent users from gaining access to information assets until they have obtained authorization from the steward.

**Note:** An individual may have more than one role (i.e. an IT employee may be a User, Custodian and Steward for certain information sets (e.g. applications, databases, files, Etc)

The roles of responsible personnel involved in the security framework for classified information sets are:

1. Owner  
Electronic information sets are owned by the Senior Vice President for the particular UCHC entity or his/her designee (i.e. Clinical, Central Administration, SOM, SODM, Research, Etc). IT will maintain a list of the owner of the information sets and any person designated to serve as the owner. The data set owner's responsibilities are:
  - Assigning the Data Steward
  - Replacing the Steward if the Steward leaves the department and notifying IS in writing of the change
  - Having detailed knowledge about the sensitivity and criticality of the classified information sets under their control
2. Steward  
The owner of each particular data set assigns a data Steward from their department. The Steward's responsibilities are:
  - Knowing and understanding the data for which they are responsible.
  - Evaluating and ensuring the data has been appropriately classified based on: State and federal law, regulatory agency requirements, and any contractual obligations; UCHC regulations/policies; and the confidentiality, criticality and sensitivity of the data.
  - Reviewing and approving, in conjunction with Information Technology application systems changes which may affect the accessibility and security of the data in their control.
  - Ensuring that the accuracy of the data is maintained.

- Working with the Information Security Officer or his/her designee, determining and approving, which classes of users should be combined into a lesser number of information access “roles”. The user will be granted access rights based on the information system needs assigned to the particular role to which their position is assigned. (i.e., physicians, RNs, clerks, accountants, lab technologists, residents, students, etc.)
- Review security violations and report to management.
- Providing written notification to IT regarding the delegation of responsibility.
- Data steward will periodically review user accesses that have been granted over a predefined period (e.g. 30 days) and follow up with the IT personnel or even directly with users whose access privileges appear inappropriate. Data steward may also review portions of audit trail data that track users accessing their datasets and investigate patterns of unusual usage.

3. Custodian

Data custodians are Information Technology personnel assigned to support the various data stewards by providing technical support and delegated task execution as appropriate. The data custodian’s responsibilities are:

- Implementing security procedures established by the data steward, including audit trail, system backup and disaster recovery tasks
- Granting access privileges to system users (e.g. a data steward authorizes a request for access and passes the operational task on to a data custodian)
- Supplying the stewards with audit trail data or other system warning about unusual or inappropriate activity
- Detect and respond to violations of policy and procedure and weaknesses in security measure
- Coordinate with data steward to propose changes to policies and technical mechanisms to enhance security
- Implement and administer controls over the information according to instructions from the steward
- Ensure proper off-site backups of critical information are made.
- IT will maintain a list of Data Stewards and the electronic records/files maintained by each.
- At a minimum of once a year, IT will coordinate a review of the Data Steward list for appropriateness and currency of assigned personnel, updating as appropriate.

4. Users

Users access data on the basis of their need to know and are obliged to comply with controls over the information as determined by particular level of classification assigned.

D) Classification Assignment Approval Responsibilities

The Information Security Officer is responsible for ensuring all applications have a classification assigned. The appropriate classification assignment approval committee at UCHC reviews the applications and their associated data sets to assign the commensurate security classifications. The approval committees are:

- Academic and Research Owned Data Sets: Computer Users Advisory Committee (CUAC)
- Clinical Owned Data Sets (Physical and Behavioral Health) – Clinical Information Technology Planning Committee (CITPC)
- Central Administration Owned Data Sets: FRS/HRS Advisory Committee

These committees will review the classification recommendations made by the owner and steward of the data set and ensure plans are in place to implement the required protective measures. Users may not be given production access to data sets meeting the criteria of classified until formal approval is received from the appropriate committee.

### III. Employee and Contractor Responsibility

It is the responsibility of each employee or contractor granted access to any of the information assets of the UCHC to exercise care in preventing exposure to any of the major security risks. Each employee shall faithfully follow the letter and the spirit of information security policies, standards and procedures and shall notify Information Security or appropriate management of any observed breach of security.

Any Person who shall access, damage, modify, destroy, remove or use information assets without authorization shall be in violation of UCHC policy and may be in violation of state or federal law. It is our policy to pursue criminal prosecution, civil action and administrative disciplinary action (up to and including termination) as appropriate to the circumstances and as allowed by law.

### IV. Security Administration

IT shall be responsible for the administration of information security policy. The Information Security Officer or his/her designee shall maintain these policies and shall establish standards and procedures for day-to-day implementation. The standards and procedures are available in the IT section of the UCHC Policy Manual and on the IT website (<http://itweb>).

Sandra Armstrong (signed)

2/4/03

---

**Chief Information Officer**

---

**Date**

Peter Deckers, M.D. (signed)

2/11/03

---

**Executive Vice President for Health Affairs**

---

**Date**

**Replaces: NEW POLICY**