HealthEast Care System	Policy and Procedure
Title: Information Ownership and Classification	**P&P #:** 106-18.2
Approval Date: 09/18/13	**Last Review Date: 09/08/14**
Effective Date: 09/18/13	**Status: Approved**

106-18.2 Information Ownership and Classification

PURPOSE

The purpose of this policy is to identify classes of information assets based on their sensitivity to the organization and to define the levels of protection needed for sensitive assets. Information assets include information systems, reports and records, electronically stored data files, system and user manuals, service agreements, and other similar items. Physical information assets include computer equipment, communication equipment, magnetic and digital media, printed information and other similar items.

SCOPE

This policy covers all data and information systems owned, licensed, or maintained by, or on behalf of, HealthEast. This includes all HealthEast information assets under the control of HealthEast or any of HealthEast's Business Associates and information assets owned by a business associate while under the control of HealthEast. A contract with a business associate may provide specific guidance for the protection and control of information assets and takes precedence over this policy in those cases.

RESPONSIBILITY

This policy applies to all HealthEast employees (including full and part-time staff), HealthEast credentialed providers, Business Associates, contractors, and other parties, who backup, store, transfer and otherwise access any information assets described in this policy.
The following individual roles are defined within this policy with the respect to the management of information assets.

Role	Definition	Responsibilities
Data Owner	Person responsible for the business results of that system or the use of the information.	• Approve access and formally assign custody of information resources. • Assign classification and specify controls based on classification to protect the information resources from unauthorized modification, deletion, or disclosure. • Confirm compliance with defined controls. • Provide appropriate authority to implement security controls and procedures. • Assure access rights are re-evaluated when a user's business need changes. • Communicates requirements to administrators for implementation and

		educates users.
Information System Owner	Person responsible for overall procurement, development, integration, modification or operation and maintenance of the information system.	• Assures implementation of technical controls for the protection of systems and data they store, transmit, or process. • Maintains the system security plan and procedures and ensures that the system is deployed and operated according to HealthEast technical control standards. • Maintains the system backup and recovery plan and ensures that business data residing on or controlled by the system can be recovered.
Data Custodian	Person responsible for the safe storage, transport and distribution of data and implementation of business rules, including DBAs, Data Modelers, and ETL analysts/developers.	• Works with data owners to gain a better understanding of and to document control requirements. • Performs audits • Ensures access to the data is authorized and controlled. • Ensures processes exist for data quality issue resolution. • Implement physical and technical safeguards to protect the confidentiality, integrity, and availability of information assets in accordance with this policy and HealthEast control standards. • Data added to data sets are consistent with the common data model. • Versions of Master Data are maintained along with the history of changes. • Change management practices are applied in maintenance of the database.
Data User	Person who receives or uses data from a system or is authorized to access information assets.	• Adheres to all HealthEast policies, guidelines, and procedures pertaining to the protection of information assets. • Reports actual or suspected security violations or information breaches to IS Security.

106-18.2.1 - INFORMATION ASSETS AND OWNERSHIP

All major information assets must be accounted for and have an owner. Owners may have responsibility for data ownership as well as system ownership depending on the size and complexity of the information system. Contact IS Security for assistance in determining these role assignments.

106-18.2.2 - INFORMATION CLASSIFICATION

Data owners must assess the value and obligations regarding data assets under their control and assign a classification. These assets must be classified as defined by the following:

106-18.2.2.1 - Confidential Information

Included in this classification are reports, records, or files containing patient, resident, or client information that is defined as protected health information (PHI), employee PHI, personally identifiable information (PII), other employee information (i.e. salary, vacation time, benefits, etc.), business strategies, HealthEast financial information (excluding information approved for release) and other similar information that is critical to the operations of the HealthEast organization. Information classified as HealthEast Confidential must be clearly identified as follows:

- All screens and printouts containing HealthEast Confidential information must be clearly labeled with the words “HealthEast Confidential”, where technically feasible.
- Appropriate controls used to protect HealthEast Confidential information from unauthorized disclosure, modification or destruction.
- HealthEast Confidential information must not be disclosed outside of HealthEast without a signed Business Associate Agreement (BAA).

Certain information protected under statutory requirements, in addition to the above controls, must be managed according to the laws or regulations governing them and will be considered **Restricted**.
Such assets include, but are not limited to chemical dependency, mental health information, genetic information and HIV status.

- Access to **Restricted** information is provided only to those with a need to know in compliance with applicable laws.
- Release of **Restricted** information requires authorized consent, legislation, or court-ordered subpoena/warrant.
- Unauthorized release of **Restricted** information may result in disciplinary action including legal consequences.

106-18.2.2.2 - Internal Use Only Information

Included in this classification are general reports and records, business memos and procedures, non-confidential email, and other information not classified as confidential or public. Information classified as Internal Use Only need not be labeled.

HealthEast Internal Use Only Information should not be disclosed outside of HealthEast without a documented business requirement.

106-18.2.2.3 - Public Information

Included in this classification are press releases and information approved for release by HealthEast's Organizational Communications department or legal counsel, non-confidential information posted on the public HealthEast website, and other similar information.
Information classified as Public does not need to meet the security controls for confidentiality and does not need to be labeled.

106-18.2.2.3 – Additional Information

To further help determine how information should be classified, please refer to **106-18.2, Attachment A, Information Classification Guidelines**. These guidelines are provided to assist Data Owners in better understanding how to classify information.

REQUIREMENTS

Relevant Knowledge: Final privacy and security regulations issued by the U.S. Department of Health and Human Services ("DHHS") pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

PERFORMANCE EVALUATION

Consequences: Security policy violations will be handled consistent with Human Resources policies (Refer to **Human Resources Policy Corrective Action, 103C.03**.) Violations may result in corrective action up to and including termination. Refer to **HealthEast Policy Information Privacy, 106-35, Attachment B**, for corrective action guidelines. Criminal violations may result in prosecution or other legal action, in addition to corrective action.

EXTERNALLY RELATED DOCUMENTS

103C.03 Human Resources Policy: Corrective Action
106-35 HealthEast Policy: Information Privacy, Attachment B
106-18.2, Attachment A, Information Classification Guidelines
106-18.e HealthEast Letters of Assignment

CONTRIBUTING AUTHORS

HIPAA Compliance Task Force

DISTRIBUTION / ROUTING LIST

Information System Owners
Data Owners

REVISION HISTORY

Date	Editor	Comment
09/08/2014	Kristi Yauch	Reviewed
09/18/2013	Kristi Yauch	Updated policy with new content
08/26/2013	Kristi Yauch	Corrected links, titles and references
06/12/2013	Kristi Yauch	Created Policy

SIGN-OFF APPROVALS

Approval Date: _____

Authorized by: _____

HealthEast - Chief Information Officer