

 YALE-NEW HAVEN COMMUNITY MEDICAL GROUP, INC.	Effective Date April 27,2004	Supersedes None	Policy Number IS1
	Yale-New Haven Community Medical Group Information Systems Security		

Purpose:

- The purpose of the Yale-New Haven Community Medical Group (YNHCMG) Information Systems Security policy is to assure that the security rules and the administration thereof exist and are consistent, as appropriate, with those developed and implemented by the Yale-New Haven Hospital (YNHH) the Yale-New Haven PHO (YNHPHO) and Yale New Haven Health System (YNHHS).

Principles:

- The YNHCMG has adopted in their entirety the principles and structure of the *Information Systems Security* policy (III.C.2) the *Electronic Communications* policy (III.C.3) and the *Confidentiality Policy (II.D.6./Type3)* of YNHHS (Attached).
- In addition to the content and intent of these policies, the following information is also true when considering security of Yale-New Haven Community Medical Group information systems.
 1. The YNHCMG supports compliance with HCFA and HIPAA regulations focused on protecting individually identifiable data from unauthorized access.
 2. The YNHCMG will undertake reasonable efforts to collect written verification from any / all vendors responsible for the collection, analysis, distribution and / or publication of data that the vendor is compliant with HIPAA regulations.
 3. Data will be used exclusively for the identification, analysis and action step planning around clinical, financial and service performance improvement initiatives related to YNHCMG business objectives and contractual obligations.

Definition:

- This policy applies to all members, employees, vendors and consultants to the YNHCMG who have direct access to confidential information via written and/or electronic medical or business records including patient care case studies and meeting materials or minutes, or hold sign-on/password identification codes to access computer systems which support YNHCMG initiatives including, but not limited to:
 - 1) Internal or External Data Warehouses
 - 2) YNHCMG Clinical Integration Initiatives
 - 3) YNHCMG Website

Procedure:

- The responsibility for administering this policy lies with the YNHCMG Board of Directors who coordinates and align their efforts with the resources designated by the YNHCMG Executive Director to administer security for systems under their control. In addition to the content and intent of procedures described in the YNHHS Information Systems Security policy (III.C.2) and Electronic Communications policy (III.C.3), the following procedures are also true when considering specific YNHCMG information systems.

Data Access and Distribution

- Access, collection, organization and distribution of data and information to be used for analysis and decision making within the YNHCMG will be at the lowest level needed to accomplish the assigned task and will be authorized by the YNHCMG / IPA Executive Director, the YNHCMG President or YNHCMG / IPA Medical Director as follows:

Temporary: YNHCMG designated and authorized consultants; Level of access to be authorized will be determined on case by case basis but will not exceed that needed to complete the assigned task(s). Access to data will be automatically revoked on completion of work, at evidence of non-compliance with the YNHCMG Information Systems Security Policy (including its references) or at the discretion of the YNHCMG Executive Director, the YNHCMG President or the YNHCMG Medical Director.

Level One: “View Only” access to aggregate, non-identifiable clinical and financial data that is typically and purposefully extracted from a larger database

Level Two: Access to individually identifiable provider financial data and aggregate member utilization data

Level Three: Access to individually identifiable provider and member financial and utilization data for specific subset of members, providers or services. Subset to be defined by the YNHCMG Executive Director, the YNHCMG President or YNHCMG Medical Director

Level Four: Unrestricted access to identifiable financial data and identifiable member and/or provider utilization data for the entire YNHCMG

Examples	Temporary	Level One	Level Two	Level Three	Level Four
YNHCMG designated and authorized consultants i.e., independent auditors, Website designers, database designers, etc.	X				
YNHCMG members at large, authorized distribution to a group to support presentation of YNHCMG / IPA program concepts or business reporting		X			

Examples	Temporary	Level One	Level Two	Level Three	Level Four
YNHCMG Board Members, Executive Director YNHCMG, President, YNHCMG, YNHCMG Contracting and Credentialing Committee members, and designates charged with managing financial performance of YNHCMG			X		
Clinical Integration Committee Chairs, Medical Directors, support staff and designates of YNHCMG subsets charged with development and implementation of specific medical and financial management initiatives related to larger YNHCMG goals.				X	
YNHCMG Medical Director, YNHCMG Medical Manager, YNHCMG Case Managers, YNHCMG Director Finance and Information, YNHCMG Data Specialist, authorized System Administrator(s) for YNHHS and approved outsourced web-based applications					X

Procedure

- Importing Information Into YPHO Internal Data Warehouse:

Partial or complete data sets that contain sensitive financial data or member, provider or service identifiable information and are received in raw or formatted form from external sources such as payers, pharmacy benefit management companies, or consultants will be imported by a YNHCMG designated Data Specialist. The Data Specialist will be responsible for recognizing information that requires restricted access and distribution and will work under the guidance of the YNHCMG Executive Director to protect member and provide privacy and secure the file(s) to the extent that is mandated by regulatory or accrediting agencies.

- Exporting Information To An External Data Warehouse:

Partial or complete data sets that contain sensitive financial data or member, provider or service identifiable information and are to be exported in raw or formatted form from an internal data warehouse source to an external data warehouse will be exported by the YNHCMG designated Data Specialist. The Data Specialist will be responsible for recognizing information that requires confidential export and will work under the guidance of the YNHCMG Executive Director to protect member and provider privacy and to secure the file(s) to the extent that is mandated by regulatory or accrediting agencies.

- Internal Standard or Ad Hoc Reporting / Distribution Of Information:

Decision making data should be provided to users at the highest level possible while still providing the essential elements of decision support detail. The Data Specialist will be responsible for recognizing information that requires confidential reporting / distribution and will work under the

authorization of the YNHCMG Executive Director, the YNHCMG President or the YNHCMG Medical Director to design and distribute hard copy or electronic reports that protect member and provider privacy and are secure to the extent that is mandated by regulatory or accrediting agencies.

Attachments:

Yale New Haven Health Policy: Information Systems Security (Policy Number III.C.2)
Yale New Haven Health Policy: Electronic Communications (Policy Number III.C.3)
Yale New Haven Health Policy: Confidentiality Policy (Policy Number II.D.6 / Type 3)

Craig P. Summers, MD
President, Yale-New Haven Community Medical Group