HIM Functions in Healthcare Quality and Patient Safety. Appendix A: Patient Safety and Quality Opportunities for HIM-IT Collaboration

Save to myBoK

In today's world, HIM staff must work together with the IT department to ensure the confidentiality, availability, and integrity of health information. This teamwork can enable safe, high-quality care and the efficient provision of services.

Normally HIM professionals are not responsible for approving or rejecting devices, tools, applications, or systems used in the course of data collection and dissemination. However, as the gatekeeper of health data, HIM professionals must be appropriately knowledgeable about data collection and dissemination methods. In that role, HIM professionals are responsible for identifying any security and data integrity risks involved with new devices, tools, applications, or systems as part of their fiduciary responsibilities to their organization.

The healthcare market is filled with products that promise efficient healthcare delivery. Organizations must assess any product for security risks before implementation. Such systems need to be analyzed for essentials such as data storage, encryption, and HIPAA compliance to ensure that data are secure.

HIM staff may not be primarily responsible for this function. Instead it is often tasked to the IT department and managed as an outsourced function by HIM professionals before recommending approval of the device.

The HIM professional is not by trade an information technologist. Therefore HIM responsibilities would encompass knowledge of devices and applications including but not limited to:

- IT components that make up the infrastructure within the confines of the domain that data serves
- Utility applications or tools that are used to capture, transform, integrate , retrieve, or alter data
- Applications used in the day-to-day delivery of healthcare
- Other applications designed to append, modify, or retrieve data

The HIM staff should be an active part of the program management and IT steering committee as applicable to ensure the continuity of information and strategy for the organization.

As matter of course the HIM professional must have, maintain, and review the following:

List of all approved input devices/tools. The review should include but not be limited to make, model, manufacturer, date put into service, calibration information, location, purpose, data protocol (e.g., Health Level Seven), connection to the system (e.g., IP address), serial port, any ancillary application required for the transfer or use of the equipment, and analysis documentation for security as needed. The following categories should be included in the review:

- One-directional lab/measurement equipment
- Bidirectional lab equipment/measurement equipment
- Bluetooth and wireless devices that can access protected data
- Scanning equipment with no data storage capability
- Scanning equipment with data storage capability including the method to protect or destroy stored PHI
- Downloadable devices such as digitizer pens
- Computer terminals including but not limited to thin clients, PC workstations, laptops, virtual desktop workstations
- Digital input devices such as cameras, imaging equipment

List of all data exchange/transformation utilities. This includes any integration applications required to transfer data to or from the protected data environment. The review should include but not be limited to manufacturer/developer, date put into service, version number, most recent update, who runs the utility application, whether the utility is operated manually or automatically, location of utility application (e.g., server or workstation), purpose, data protocol (e.g., Health Level Seven),

any ancillary items required to run the utility application (e.g., a copyright dongle), application required for the transfer or use of the equipment, and any documentation or overview of the utility application.

List of all manual data exchange/transformation functions. This includes any spreadsheet manipulations, automations, or reports manually prepared to be reinserted into the protected data environment. The review should include but not be limited to the person who developed the process, process documentation, process platform (e.g., Excel), date put into service, most recent update, who runs the utility application, location of utility application (e.g., server or workstation), purpose, any ancillary items required make the data exchange/transformation, and any documentation or overview of the utility application that may require an interview.

List of all passive data retrieval methods. This includes any application, function, utility that retrieves data from the protected environment with no connection or means of altering the protected data or saving updated information. This includes automated processes.

The review should include but not be limited to the person who developed the process, process documentation, process platform (e.g., Excel), date put into service, most recent update, who runs the utility application, location of the service, and means of view (e.g., Web portal). The following categories should be included in the review:

- Business Intelligence systems including dashboards
- Automated reporting services
- SQL reporting service, Cognos, Performance Point, etc.
- Excel-connected spreadsheets
- Web-enabled reporting
- Data transfer services
- Shared data services with outside sources such as an HIE
- Proprietary reports to other facilities
- Data integration into other applications
- Electronic filing or transmission

Security documentation for the infrastructure. This includes any strategy, tactical plans, projects, issues, roles, and security matrix documentation. The review should include but not be limited to IT security personnel information, process documentation and policies, date put into effect, most recent update and audit, and most recent HIPAA survey/audit. It should include the following categories in the review:

- Methods of authentication, password, or biometrics
- Security protocol and management structure
- Data breach process and documentation
- Security matrix of access method to role, user, or group
- Copy of executed business associate and nondisclosure agreements

Audit functions within the items defined within this document. This includes the agreement between IT and the HIM personnel to utilize tools that allow the HIM personnel to interrogate the system for inappropriate or unauthorized devices. This would include the standard naming conventions as well as other IT infrastructure security best practices not addressed within the scope of this document. The review should include but not be limited to the following:

- Unauthorized equipment based on equipment name or IP address
- Security breaches or attempts
- Password hacking
- Survey or observation (unattended open data)
- Data transmission bandwidth as a tracking function out of the normal

Contact list of critical personnel. This includes but is not limited to critical IT personnel, business unit representatives, corporate security and compliance personnel, and local, state, and federal offices.

Document files including but not limited to the following categories

- Requests for data, reports, etc.
- Data formats accumulated internal and external, such as HL7, ASTM, etc.
- Data dissemination and reporting practices

- Internal data format and design requirements
- Data service agreements such as to outside organizations or other institutions
- Data code set information for the analysis and of data attributes

For HIM professionals who want to combine their HIM background with IT functions, potential careers can be found in areas such as enterprise applications specialists, integration architect, or clinical applications coordinator.[1] HIM practices lend themselves to a successful future in health IT roles.

Note

1. AHIMA. "HIM and Health IT: Discovering Common Ground in an Electronic Healthcare Environment." *Journal of AHIMA* 79, no .11 (Nov.–Dec. 2008): 69–74.

Back to practice brief

Article citation:
AHIMA. "HIM Functions in Healthcare Quality and Patient Safety. Appendix A: Patient Safety and Quality Opportunities for HIM-IT Collaboration." *Journal of AHIMA* 82, no.8 (Aug 2011): expanded online version.