DATA SECURITY AUDITS

Chris Apgar, CISSP
President, Apgar & Associates, LLC
10730 SW 62nd Place
Portland, OR 97219
capgar@easystreet.com

Table of Contents

DATA SECURITY AUDITS

¶100 INTRODUCTION

When we think of audits we generally think of a visit from the trained professional who pours over reports, processes, facts and figures. The dreaded visit from the auditor is often perceived as something to be feared — the fear of exposure, the fear of mistakes printed in bold in a report forwarded to senior management or, in the worst case, fear of employee wrongdoing of a criminal nature. The purpose of this chapter is to dispel a few myths (no auditors don't need to be viewed as the grim reaper waiting to pounce) and highlight the positive outcomes of a quality audit.

For the auditor reading this chapter, if you are searching for a step-by-step approach using proper audit techniques for security audits, you will likely not find what you are in search of. The focus will be from the vantage point of a practitioner, the one who arranges the audit, lays the groundwork, and follows up on noted deficiencies. Plenty of material exists defining appropriate audit practices, but most articles and texts are focused on what the auditor needs to know and not what those within an organization need to prepare for and engage in an audit process that assists in strengthening security and privacy protections.

In addition to extolling the virtues of data security audits and focusing on the needs of non-auditors, this chapter outlines the new regulatory requirements regarding data security audits. One of the many gifts presented to the health care industry from HIPAA's Administrative Simplification Provisions is the need to actually examine practices and safeguards on a regular basis. There are a number of ways to go about the job of auditing processes and this chapter will attempt to address needs that will vary depending on the size of the organization and its primary business functions. ➢➢

¶110 HIPAA Data Security Requirements

The HIPAA data security rule requires organizations, at a minimum, to conduct periodic internal audits to evaluate processes and procedures intended to secure

confidential or "protected health information" (PHI)(§164.308(a)(8)). It is often advisable to seek an external review or audit but the provisions of the data security rule do not specifically require this. In most cases, this will be determined by the size of the organization, line of business, and, sometimes, contract requirements (i.e., Medicare, Medicaid, etc.). The purpose behind the audit is to determine if an organization has properly documented data security practices, policies, and procedures and generally meets the requirements of the rule.

An internal audit defines the process of determining an organization's compliance. To support such an audit the rule describes what needs to be maintained to support such an audit. One of the underlying requirements of the HIPAA Administrative Simplification provisions is that documentation is the key to proof of compliance. In addition, documentation defines for the organization processes that need to be followed to ensure member/patient PHI is not inappropriately released or easily accessible to those who do not have authorized access.

Section 164.312(b) of the final security regulation requires covered entities to establish audit controls that record and examine activity in information systems that contain electronic PHI. Audit trails are one part of these controls and are used to document access to data, changes or additions to records, sometimes physical access to a secure facility, etc. An important part of any audit is a review of who accessed what and what modifications were made. This is needed to make sure access is appropriate, data is protected against inappropriate viewing or modification, and procedures/processes are being followed — all of which are sound business practices.

An audit trail is merely a listing or a catalog of actions taken. Tools or audit controls are needed to sort through what can be an intimidating and, in aggregate, useless mound of data. Audit controls assist the auditor and the practitioner in keeping an eye on ongoing activity as well as background for that snapshot that is a full-blown audit. Audit controls also are a required technical safeguard in §164.312 of the final HIPAA data security rule.

The HIPAA privacy standard also requires covered entities to track access to PHI when disclosed for purposes other than treatment, payment, and health care operations for six years (§164.528(a)(1)). This indirectly relates to data security and possible audits, but it demonstrates the importance of audit trails. Regulatory, legal, and operational requirements combined should compel organizations to track who uses PHI and for what. HIPAA is just another reason to adopt sound data security practices and methods of validating protected data are truly "safe."

It is important to remember that, while HIPAA mandates audit-related activity, data security, as with financial audits, represents sound business practice. Organizations need to take heed of regulatory requirements, but such requirements need to be viewed in the context of your organization's culture and business needs. In other words, regulatory requirements need to be heeded, but if they are not viewed in the business context and are taken too lightly or seriously, the organization is adversely impacted. Heeding the demands of government at the expense of the business generally can have unfortunate and sometimes disastrous results. Audits need to satisfy the statutory and regulatory requirements. They also need to serve as tools to further the strategic goals of an organization and not become so onerous that they get in the way of what amounts to what the organization "does for a living." ➢➢

¶120 Determining Audit Needs

Before determining audit criteria (i.e., what is important to look for when evaluating the effectiveness of data security programs), an organization needs to draw a proverbial picture of itself. This includes evaluating data security requirements and how they mesh with the business. It also includes conducting a risk assessment — where are the holes and what liabilities they represent. There is no such thing as risk-free business operations.

How to properly conduct a risk assessment and gap analysis, critical parts of the foundation of a sound data security audit program, are described in Chapter 1000. Let it suffice to say that, before outlining what needs to be included in an effective audit, organizations need to identify what to look for or what areas of risk pose the most danger to the business. Also, businesses need to map their existing data security program and processes. It is difficult, if not impossible, to develop an effective audit program without knowledge of the risks to the business, mitigation activities and how the data security program is designed to effectively operate to protect the interests of the business. ➢➢

¶130 Developing an Effective Audit Program

After clearly documenting program structure and needs, the process of developing an effective audit program can begin. An effective audit process will be designed to periodically evaluate whether an organization is managing risk, adhering to established policies, and meeting the regulatory requirements of the industry (and this includes much more than HIPAA). Assuming an organization has evaluated risks, mapped out its data security program, and framed it within

the regulatory and operational context of the business, the question is "Where do we go from here?"

¶131 The Audit Checklist of Program Components

The first and most important step in building the foundation for an audit program is to develop a list of program components, associated risks, and regulatory requirements; in other words, what needs to be measured and how. When the audit snapshot is completed, that picture should show what still needs to be fixed or better enforced. Again, an audit needs to be viewed as a tool to improve security operations and not an event to be dreaded because deficiencies may be discovered.

Figure 5531–1 is a simple example of a checklist that will assist in framing what an audit program needs to include and, in some cases, who should conduct the audit (internal versus external audit).

FIGURE 131–1 TEMPLATE FOR A DATA SECURITY RISK ASSESSMENT

This figure provides a template for the completion of a data security risk assessment. Such an assessment should be completed prior to developing audit criteria to be used by internal or external audit resources.

Data Security Risk Assessment **Date:**						
Identified Risk:						
Level	**Likelihood of Occurrence**					
	Low		Medium		High	
Low						
Medium						
High						
Notes:						

Action	
Low/Low: No audit/mitigation	Low/Medium: Possible audit/mitigation
Low/High: Possible audit/mitigation	Medium/Low: No audit/mitigation
Medium/Medium: Possible audit/mitigation	Medium/High: Audit/mitigation
High/Low: Possible audit/mitigation	High/Medium: Audit/mitigation
High/High: Audit/mitigation	

Definitions:

Identified Risk: The specific risk being assessed (i.e., inappropriate access, data corruption, physical security breach, etc.).

Level: The level defines the amount of risk. This could include risk of inappropriate disclosure through interception, individual access, etc. It could include the likelihood of failure leading to corruption of critical data. It represents any defined risk that exposes the organization to legal or operational exposure and/or endangers your organization's stewardship responsibilities.

Likelihood: The possibility the risk assessed will occur.

Mitigation: The steps to be followed to reduce or eliminate the identified risk.

Comments:

¶132 Developing the Audit

Once the "what to look for" has been defined, an organization can develop an effective audit program and determine whether it has sufficient knowledgeable internal resources to conduct periodic audits to assist in minimizing risk. Also, an organization can begin developing an audit program that succeeds in documenting adherence to sound business practices and meets defined regulatory requirements.

The breadth of the audit and its frequency should be defined by business and regulatory needs and not a boilerplate program that may generally meet so-called sound audit practice but not necessarily the specific needs of an organization. Standardized audit processes are valuable (as long as they remain at least somewhat industry-specific) because they generally have been developed with sound business practices in mind and have been demonstrated to be effective in the "real world." But they represent only a starting place. Standard practices need to be tailored to the individual needs of an organization that would include not only business and regulatory requirements but also such things as organizational culture and size. As an example, an audit program for a large health delivery system will likely not be appropriate or effective for a medium-sized health plan.

Standardized audit programs exist across industries and, in many cases, have been tailored to the needs of each industry. As an example, the National Committee on Quality Assurance (NCQA) has developed a standard set of criteria and requirements that are used to determine not only the effectiveness of a data security program but also important components of such a program. It is always wise to start with an already developed and accepted standard (as long as it is also industry-specific). It is not necessary to reinvent the wheel.

It is also a good idea to evaluate more than one standard audit process to determine the best fit. After determining best fit, a standard audit program or process can be tailored to meet the specific needs of the organization by comparing standard criteria against the previously developed roadmap outlining organization specific risks and needs, processes and culture, etc.

Figure 5532–1 is an example of a standard audit process that is specific to health care. It may form the foundation of the tailored approach recommended in this chapter. This sample audit checklist is based on the specific criteria included in the final HIPAA security rule. (Because the requirements in the final security rule were not as specific as the proposed rule, some of the details of the proposed rule are still useful to evaluate a data security program and have been included.) Again, specific audit criteria need to take into account your organization's

business, culture, environment and other factors that impact your operation. There are many formats developed specifically for a variety of industries. A number have been modified and are being distributed as appropriate to health care. This is not always the case. Returning to the risk assessment when determining whether a given set of criteria or audit program is appropriate for your organization is most appropriate at this time. You may find the template suits your needs, but you may also find that adjustments are needed.

133 Criteria into Something Measurable

Figure 133–1 is an example of how audit criteria are transformed into something measurable. It is relatively easy to identify areas of concern or risk that should be scrutinized during an audit. However, it takes a bit of time and effort to develop the detailed steps to be followed when conducting an audit to determine whether criteria, or what your organization feels is important to examine, adhere to sound data security practices and minimize organizational and legal risk. Figure 5533–1 is an example of one of the many detailed guides available. The model is excerpted from the Treasury Board of Canada Secretariat ("Audit Guide — Information Technology Security," September 1995). It may be downloaded from www.tbs-sct.gc.ca/Pubs_pol/dcgpubs/TB_H4/ 01GUID_e.asp.

FIGURE 133–1 AUDIT GUIDE
Excerpted from Treasury Board of Canada Secretariat, Audit Guide — Information Technology Security, September 1995)

Objective #1

Ensure that an Information Technology Security management structure is in place and meets the needs of the department.

Criterion 1.1 – Security management responsibilities are established, defined and assigned.

Detailed Criteria/Audit Procedures:

1.1.1 Obtain a copy of the most recent departmental security organization chart(s). Determine its adequacy in portraying all security relationships (both line and functional).

1.1.2 Determine whether a senior official has been formally appointed to represent the deputy head in dealings with the Treasury Board Secretariat on matters concerning the security policy and standards.

1.1.3 Determine whether a Departmental Security Officer (DSO) has been formally appointed by the deputy head and if the DSO position is sufficiently senior.

1.1.4 Determine whether an information technology systems (ITS) Coordinator has been formally appointed and if the ITS Coordinator has at least a functional relationship with the DSO.

1.1.5 Determine whether a separate position for a Communications- Electronic Security (COMSEC)

1.1.6 Authority has been formally appointed, or if the Communication Security Establishment (CSE) has been appointed to act on behalf of the department. Assess whether the working relationship of this position with the position of the ITS Coordinator is appropriate.

1.1.7 Review the key ITS position descriptions to determine if the required duties and responsibilities have been included. Determine whether the position descriptions reflect the current organizational needs. Determine what priority and percentage of time is allotted directly to security related duties.

1.1.8 Interview key ITS personnel on their knowledge of the security requirements of their positions. Determine the actual percentage of time spent on ITS matters and compare with that in the position description.

1.1.9 Interview selected middle and senior responsibility center managers, who are responsible for significant IT, such as critical local area networks (LANs), wide-area networks (WANs), or traditional data centers, to determine their knowledge of their ITS responsibilities. Determine if their position descriptions include ITS duties and responsibilities.

1.1.10 Interview select LAN/WAN/data centre managers to determine their knowledge of their ITS responsibilities. Determine if their position descriptions include ITS duties and responsibilities.

Criterion 1.2 – An ITS planning process is in place.

Detailed Criteria/Audit Procedures

1.2.1 Obtain copies of past security audits, management self-assessment reviews, security program reviews, internal security reviews, RCMP Security Evaluation and Inspection Team (SEIT) reviews, CSE reports and any other related security reports.

1.2.2 Determine whether there is a formal plan for ITS for the current fiscal year or whether it is a sub-set of the overall security plan. Determine whether the plan was developed in concert with, and in consideration of, other critical departmental plans and reports, such as: overall security plans; IT plans and strategies; information management plans (IMPs); the departmental business plan; RCMP SEIT reports; CSE reports; and inter-departmental ITS committee recommendations.

1.2.3 Review the level of funding of ITS in relation to the level of funding for IT. Consider the implications of any significant changes in the level of funding and whether the level of funding is adequate.

1.2.4 Examine the plan for completeness, reasonableness of its time frames, adequacy of resources (including financial, personnel, and information) and authorization.

1.2.5 Ensure that the plan addresses the implementation of the security policy, and the ITS standards.

1.2.6 Ensure that the plan addresses the management-accepted recommendations of past security audits and reviews.

1.2.7 Verify that the plan addresses the requirement for developing contingency plans to restore computer operations following an interruption within the specified time as set out in the statement of sensitivity.

1.2.8 Verify that the plan considers the whole of the organization's ITS needs such that it would create economies of scale (*e.g.* acquisition of computer virus software or laptop computer access control software).

1.2.9 For interdepartmental activities requiring Treasury Board submissions for IT systems, determine whether other potentially affected departments were provided the opportunity to help formulate security plans.

1.2.10 For departmentally shared IT systems, determine whether the other departments were afforded the opportunity to jointly assess threats and risks, agree on security requirements, safeguards, terms and conditions.

1.2.11 For departmentally shared IT systems, determine whether security terms and conditions are agreed to in a Memorandum of Understanding.

Criterion 1.3 **– Necessary functional linkages exist.**

Detailed Criteria/Audit Procedures:

1.3.1 Determine whether internal linkages exist between the ITS function(s) and other administrative functions in the organization, such as:

- EDP and/or telecommunications organization(s) (if separate from ITS)
- IT outsourcing contractor
- Information management (if separate from ITS)
- Materiel management
- Property management, and
- Personnel management

1.3.2 Verify whether the ITS Coordinator has instituted a distributed network of formally appointed, local, part-time, ITS officers (for example, LAN Administrators formally appointed as local ITS officers, and having their ITS duties incorporated into their position descriptions). Verify if the network is kept current.

1.3.3 If an ITS personnel network exists, interview select local ITS officers.

Determine the extent to which they are given adequate direction and support from the ITS Coordinator. Assess if they know (and work with) their local physical security/personnel screening officer (if similar personnel networks exist).

1.3.4 Determine the extent to which the ITS Coordinator participates in intra-departmental IT committees, working groups, and projects. Determine the level of visibility the ITS function has in each of these committees, groups and projects.

1.3.5 Determine whether external linkages exist between the ITS function(s) and outside agencies such as:

- Royal Canadian Mounted Police (lead security agency)
- Communication Security Establishment (lead security agency)
- Canadian Security Intelligence Service (for specific threat assessment information) and
- Emergency Preparedness Canada (for specific emergency planning information)

(Contact the two lead ITS agencies. Determine their involvement in the ITS activities of the organization being audited during the past several years. Determine whether departmental units contact the lead security agencies directly and if the ITS Coordinator is aware of all security lead agency involvement in the department.)

1.3.6 Determine the extent to which the ITS Coordinator participates in inter-departmental ITS committees such as the Information Technology Security Committee (ITSC) and the Communications-Electronic Security Committee (CSC).

1.3.7 Determine if committee representatives are appropriate. Consider the technical expertise of representatives, experience in such roles, and authority levels of representatives.

¶134 Deciding Who Will Be Responsible for the Audit Program

After developing a specific set of audit criteria and deciding how that criteria will be utilized during the audit process, the time has arrived to determine who will accept responsibility for administering your audit program. While internal audits may be sufficient, you may choose to seek external assistance or combine approaches. Again, this will depend on your organization. As an example, it is probably not cost-effective or necessary to contract with an external consulting firm to conduct a data security audit if your business is small, employs few staff

and relies primarily on paper-driven processes. Internally versus externally managed audit program details will be addressed later in this chapter at ¶5550. ➢➢

¶140 Developing a Plan for Implementation

Now that you have the criteria identified, where do we go from here?

Before involving the organization in the implementation process, it is wise to develop a plan for implementation. An audit process is structured and usually based on accepted standards. A trained internal or external auditor can assist in providing the structure needed to operationalize an audit program but not necessarily implement the program. Establishing the program must be treated as any other project and must be appropriately managed to ensure time lines are followed, the needed resources available and the criteria matches organizational practice. Here is a listing of some of the steps that need to be considered, which is not all-inclusive and will vary from organization to organization:

- Complete risk assessment and gap analysis.
- Review existing industry standards and develop or amend existing processes and policies to support sound data security practices.
- Review existing industry-specific audit criteria and determine appropriate criteria for your organization.
- Develop related training programs (general and targeted) and a training schedule. (This should not be a one-time event.)
- Implement training programs, including the communication of established audit criteria.
- Develop an audit schedule or schedules. (There may be a need to conduct a general audit annually but targeted audits at more frequent intervals.)
- Develop documentation identifying the relative weights associated with audit criteria (i.e., it is more important to address a potential audit finding that indicates the organization's web site is vulnerable to penetration versus a password problem with one device that is not used to store sensitive information).
- Develop templates for communicating audit findings and suggested solutions to problems identified through the audit process.
- Develop a process for findings follow-up (i.e., following through with responsible management, tracking findings and implemented solutions, etc.).
- Communicate the audit schedule to affected management and staff.
- Implement a structured audit program.

- Conduct audits according to the established schedule and communicate findings in an established fashion.
- Schedule a review of the audit process following a complete cycle to evaluate the effectiveness of the audit program.

¶141 The Need for Involvement by Senior Management

An audit program is only as good as the knowledge base of the organization. In other words, risks need to be communicated, policies circulated and understood, training conducted and audit criteria relayed to those in your organization responsible for managing programs or processes to be audited. If responsible management is aware of what is required and what will be looked for in a compliance audit, the likelihood is greater that risks will be mitigated and appropriate practices implemented and followed.

After completing a risk assessment and defining audit criteria, it is good practice to first involve senior management, followed by affected staff. The purpose of an audit is to assist an organization establish and follow acceptable practices. For an audit to be successful, for audit findings to be acted on, it is necessary to solidify top-down support. If top management is not committed to enforce good practices, and to dedicate the appropriate resources to address deficiencies identified during the audit process, it is likely that data security will continue to be a lower priority and risks that should be mitigated will continue to exist.

One of the better methods of gaining senior management support for implementation and operalization of an audit program is to sell senior management on the merits of the program. This could include the following:

- Document the return on investment (ROI) (i.e., increased customer satisfaction, cost avoidance from litigation that doesn't materialize, etc.).
- Provide a "sound bite" overview of regulatory requirements and best practices (i.e., keep it short and to the point).
- Research and present what competitors are accomplishing that may provide them with a more favorable market position related to data security and privacy activity (i.e., a significant competitor acquiring a secure messaging solution that can be used by customers to protect privacy, increasing the satisfaction and comfort of the customer).
- Walk through a short list of high level risks, events that are likely to occur or would be expensive if the risk is not mitigated.
- Provide examples of breaches in other organizations in your industry , but be

careful to use "scare tactics" sparingly, since they can be met with responses like "that has never happened to us," or "you're playing Chicken Little again."

- Provide a high-level implementation plan with needed resources to implement and operationalize it.

Garnering senior management buy-in is not a one-time event. It is highly likely that you will be required to present your case to senior management more than once and in different ways before solid support materializes. Your audience assimilates information differently, hence the need for multiple communication vehicles. Also, while generally the need for data security and privacy protection are seen as important, it may require at least some "selling" to place data security on the same level of importance as other priorities, such as e-health initiatives or developing a new product or service.

In some respects, selling to senior management also will also become a part of the audit process. Significant audit findings will require action on the part of the organization. Allocating the resources or directing existing resources to address findings will require the support of senior management, as well as operational management. In some cases audit findings will require a significant investment of resources (i.e., acquiring an intrusion detection application, assigning additional staff to manage access to information, etc.). In most organizations, resources are scarce and there are many priorities. Data security becomes a priority only when ongoing activities keep the message in front of top management.

¶142 Training Operational and IT Management

The next step in implementing a sound audit program is training of operational and information technology management, as well as affected staff. This may require stepping back and providing basic data security training, re-familiarizing management and staff with existing policies, and providing targeted training to groups identified as needing a higher level of training (i.e., network administrators, medical management case workers, etc.). It is difficult if not impossible to obtain support for an audit program if management and staff lack the training necessary to understand the need. Refresher (or in some cases new) training assists in providing the "whys" and, where needed, the "hows."

The success of an audit program (i.e., how well it is received, how successfully it resolves audit findings, etc.) is only as good as the knowledge of the participants — management and staff. Auditors are often seen as intrusive and "out to get you," but this viewpoint does little to support successful audit program

implementation and management. If management and staff understand the basic risks and processes to address risks, and the reasons behind the audit program are explained in sufficient detail, this negative image of auditors will be less likely to hamper sound audit practices.

¶143 Sample Data Security Policy

Figure 5543–1 is an example of a concise data security policy that can serve both as a training tool and as something to point to when attempting to convey audit results to management and staff. It is part of the necessary foundation, a piece that needs to be communicated and understood, before a successful audit program can be rolled out. This example from the State of New York was selected because of its brevity, which lends itself to easier communication to management and staff and less ambiguity when it comes to enforcement or, in this case, completion of an audit.

FIGURE 5543–1 SAMPLE DATA SECURITY POLICY

State of New York

Information Security Policy (Technical Policy 97-1)
January 9, 1997

Statement of Purpose
This document is designed to provide State agencies with recommended *minimum*-security policies for protection of assets inclusive of information, computers, and networks. These are high-level statements, independent of technology, designed to provide broad direction and goals. A companion document of standards and best practices is currently being drafted to supplement these policy statements and to provide guidance for implementing these recommended security policies. In advancing this policy, it is understood that individual business needs and requirements of individual agencies may justify changing certain components of this policy. Changes should only be made after careful consideration and consultation with the procedures and best practices companion guide. This policy should be applied to all existing and future technology infrastructures.

Information Custodianship
Information, such as data, electronic mail, documents and software, are agency assets. In determining the value of an asset, consideration should be given not only to the sensitivity of the information, but also to the consequences of unauthorized disclosure, modification, destruction, or unavailability of the information. The value of these assets will determine the level of controls needed to provide adequate safeguards, backup and

access controls. However, ownership, custodial responsibility and rights to these assets must first be established.

Agency Records. A "record" includes any information kept, held, filed, produced or reproduced by, with or for an agency in any form or media including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, images, photos, letters, microfilms, computer tapes or discs, rules, regulations or codes.

Property of an Agency. All records, software, and hardware that are part of an agency's information system are considered property of the agency and should be used for agency business purposes only. In furtherance of a governmental purpose, an agency head or designee has the right to examine all information residing in or transmitted by means of agency communications or computing devices.

Designation of Responsibility. An agency head or designee has the ultimate responsibility to ensure that all agency information resources, regardless of medium, are used, maintained, disclosed and disposed of according to law, regulation or policy.

Copyright and Licensing of Vendor Hardware and Software. Agencies must adhere to copyright laws and licensing agreements.

Records Retention and Destruction. Agency information must be retained and/or destroyed in accordance with records retention schedules developed in cooperation with the State Archives and Records Administration (SARA) and policies and procedures established by the agency, unless required otherwise by applicable laws.

State and Federal Access, Privacy and Confidentiality Laws. All information, regardless of the medium in which it is maintained or communicated, is subject to pertinent State and federal laws governing access, the protection of privacy and prohibitions against unauthorized disclosure.

Access Categories. Classification of Information. Information classification provides a means for separating information into categories with different protective requirements. Agencies should determine, in advance, the extent to which information should be disclosed to specified users. Determinations should be made based on the nature of the information and the duties of agency employees. The following general categories of information serve to provide guidance in identifying appropriate users or recipients:

Public Information is information accessible under Freedom of Information Law and is available to any person, notwithstanding one's status or interest.

Restricted Information pertains to information which is not public information, but can be disclosed to or used by agency representatives to carry out their duties, so long as there is no legal bar to disclosure.

Confidential Information is information which is protected by law. Access to confidential information is prohibited unless permitted by an exception in law.

Physical Access Security

The agency shall put into place appropriate safeguards to limit physical access to any computer or computer related device.

Secure Locations. Mainframe, servers and other essential computer devices shall be stored in a location that protects them from unauthorized physical access. Physical access to such equipment potentially provides access to information stored therein.

Location Selection. Physical locations for all computer related equipment should be selected to protect against equipment and information loss by flood, fire, and other disasters, natural or man-made.

Review of New Connections to Outside Sources. Proposed access to or from a network external to the agency must be reviewed and approved by the agency head or designee prior to establishment of the connection.

Review of Installation. Installation, upgrade, changes or repairs of computer equipment and computer related devices (hardware, software, firmware) must be reviewed by the agency for potential physical security risks.

Platform-specific Physical Security. Platform-specific physical security must be established, implemented and periodically reviewed and revised as necessary to address physical vulnerabilities of that platform.

Laptop, Notebook and Portable Computer Devices. Portable computing devices must not be left unattended at any time unless the device has been secured. When traveling, portable computers should remain with the employee's carry-on hand luggage.

Information Security

The agency is responsible for the security of all agency information resources regardless of medium. Agency specific procedures developed to conform with the following policies must be reviewed frequently to reflect changes in personnel and technology.

Information Security Administration Functions. Each agency must formally delegate responsibility for all information security matters. Multiple individuals across organizational lines may be involved as long as there is a clear separation of duties and responsibilities which provide effective checks, balances and accountability. For example, the individual responsible for systems security should not be a system administrator whose primary responsibilities are for maintaining and upgrading operating systems. Separating systems administration from security duties improves the security climate.

Lines of Communication. Lines of communication and responsibility for

agency security must be established, maintained and clearly defined. Alternative paths must be available in the absence of one of those individuals designated in the communications chain.

These lines of communication must work in both directions either for the reporting upward of information security problems or the downward communication of problem awareness such as information security alerts, potential virus threats and the like.

Logon Security. Access to computer systems requires identification and authentication. Any exceptions to this rule require appropriate agency approval.

Remote Access to Agency Information. Remote external access to an agency network which contains restricted or confidential information requires extended authentication procedures. Any method for providing this remote access (*e.g.*, modem, firewall) requires agency approval prior to its installation.

External Network Access to Agency Information. External network access to an agency network which contains restricted or confidential information requires at least a firewall. Firewalls provide network security similar to the installation of a perimeter security system on a building by blocking or permitting traffic.

Transaction Controls and Database Security. Transactions entered into the agency's production databases must be checked for accuracy and authenticity.

Database management systems (DBMS) shall implement security and authorization subsystems adequate to protect against unauthorized access and modification.

Downloading Software. Each agency must determine whether it will allow downloading of software from an external site. Agencies that allow staff to download software must establish and follow procedures that ensure such software is adequately examined for undesirable effects before it is installed on agency machines. (Note: Agencies should be cognizant of incidental, unsolicited, or automatic downloading of executables by accessing an external site.)

Non-Agency Owned IT Components. Each agency must develop procedures for defining use of non-agency owned computer hardware and/or software for agency business. In the case of software, vendor copyright and licensing agreements must be strictly adhered to. At the end of such use, all agency information must be removed.

Agency Owned IT Components. Agency hardware should be reviewed and cleansed (sanitized) before being reassigned or discarded. Agencies should maintain adequate documentation of hardware/software taken off-site by employees.

Electronic Communications. When transmitting confidential information on an external network, agencies shall employ a technology rendering the information unusable to an unauthorized or intercepting third party.

Virus Protection. All agency computers should be equipped with up-to-date virus protection software.

Agency Security Management
Accountability and appropriate separation of duties and responsibilities are essential elements of security administration. In addition, agencies must develop security awareness among all staff, which include descriptions of practices intended to circumvent agency security management.

Security Training. All employees, agents and others who access agency computer systems must be provided with sufficient training and supporting reference materials to allow them to properly protect agency information.

Employment Changes. Managers must report changes in employment status or job duties of their staff to the information security administrator. Personnel reports regarding employee status changes must be regularly provided to the designated information security administrator.

Audit Trails. The agency must maintain audit trail records sufficient to meet the requirements of the law, the needs of the agency's internal controls and audit requirements, control agency audit requirements and, as necessary, disaster recovery requirements.

Logging. All access to networked systems must be logged. When determined to be critical to an agency, the logging of transactions must be included regardless of the operating platform. Log data must be classified as restricted. These logs must be retrievable through clearly defined procedures and must be maintained for time periods prescribed for audit, legal and recovery purposes. As new applications, platforms, mediums or other technical changes to system operations are made, consideration of logging requirements and availability must be made. Requirements for logging data must be clearly established as system, architectural, technical or network designs are developed.

Information Recovery
All systems must have back-up and recovery procedures that are

documented, maintained and stored off-site. The agency should make every effort to test these procedures on an annual basis.

Theft of Information. An agency must take measures to prevent the theft of agency information resources.

Data Exchange Agreements

Agency Agreements. Agencies with systems that exchange data with/to any other entity must sign a formal agreement with that entity to adhere to specific agreed-upon security protocols related to data exchange (see Technology Policy 96-19 - Data Sharing Among Agencies).

Third-Party Agreements. All agreements with third parties such as vendors, other government agencies, or contractors must include requirements to adhere to agency information security policies.

Vendor/Contractor Agreements

All vendor agreements shall contain a requirement that any agency information obtained as a result of such an agreement shall be the property of the State and shall not be utilized, including but not limited to secondary release or disclosure, without written authorization of the agency.

Employee/Agent Responsibilities

As a condition of continued employment, all employees/agents must sign an information security compliance agreement annually indicating that they have read and understand the agency's policies and procedures regarding information security, and must agree to perform their work according to such policies and procedures.

Password Protection. Employees/agents must not post or share their personal passwords, and must develop secure passwords not likely to be guessed.

Use of Automatic Logons. Employees/agents must not facilitate any logon procedure with local programming such as keyboard programming or scripting.

Unattended Computers. Unattended computers must be logged off or protected in such a way as to protect the computer and network from unauthorized access.

Reporting Suspicious Events. Any observations of suspicious activity must be reported to the appropriate agency representative. Suspicious activity can include: signs of unauthorized equipment usage during evenings and weekends, phone requests from unidentifiable callers for access to secure information, unidentifiable files found on file servers, and unusual activity recorded in log files.

¶150 Implementing Your Audit Program

At this point, you have understandable data security practices and policies in place, audit criteria selected, and a receptive organization. In many cases it is not as easy as that and, as noted earlier, this is not a static process to be reviewed or implemented once. But organizations are in a better position to successfully implement and administer an audit program if the foundation has been built and the processes and communication channels are in place to address the "hows" and the "whys."

Once your program has been developed and communicated, it is implementation time. If your program has been carefully developed and is appropriately structured, implementation becomes just another step in a carefully planned process. The question to answer (and hopefully you've answered it before implementation time) is who will conduct the audit — internal audit staff, a third party or a combination of the two? The answer to this question depends on the size of your organization and specific needs.

¶151 Internal Audit Staff

Many organizations think of their internal audit staff as a specifically designated individual or department charged with managing an internal audit program that usually runs the gamut from financial to compliance to operational process. This is more likely the case in medium to large organizations. Smaller organizations are more likely to employ someone who wears many hats, one of which includes general audit responsibilities. It is not feasible, nor does it make sound business sense, for a small organization (that, say, employs five staff) to designate an individual as a full-time internal auditor.

The use of an internal auditor, or the designation of an individual to perform this function on at least a part time basis to conduct data security audits, may be appropriate given the size, complexity, regulatory requirements, and needs of an organization. It is also often the less expensive option of the two (use of internal versus external auditors). Often organizations that utilize an internal auditor do so because of cost savings, the presence of available staff and/or the added flexibility of staff use (i.e., an external auditor is not always available when needed for *ad hoc* audit functions and tends to be costly if utilized for more than an annual generalized audit). Internal auditors, though, are not without their detractors and drawbacks.

It needs to be noted that internal auditors are ultimately employed by the organization. While many are fully accredited and adhere to a high code of

ethics, sometimes an audit will overlook operational deficiencies unintentionally due to perceived pressure from other parts of the organization or through familiarity. It is not uncommon for an employee to miss what may be obvious to an external party due merely to proximity. All have a tendency to miss problems or minimize risks when too closely associated with a work process.

That said, there can be significant advantages to utilizing an internal auditor. Sometimes proximity also brings with it the added value of intimate knowledge of the organization. To perform a thorough audit that is also useful to an organization, third-party auditors will have more of a learning curve to understand the specific processes of an organization. The internal auditor will also be in a better position to know the history of employees and process origins, and will have ready access to more unbiased data. Also, a number of internal auditors are nationally certified and required to adhere to rigorous standards when performing compliance or financial audits. This helps to minimize the bias or "blindness due to proximity" that can arise when an internal auditor is an employee of a given organization.

It is often wise, but not always feasible, to use both internal and external auditors for a review of data security practices. A rigorous program and the use of qualified staff (as well as following-through with training and policy maintenance) can satisfactorily meet the needs of an organization as it strives to engage in data security best practices and to minimize risks.

¶152 External or Third-Party Audit Staff

There are many qualified individuals who, for a fee, are available to perform an unbiased audit of an organization's data security practices. A quick search of the web, or better yet a phone call to a trusted colleague, is all that is required to locate a quality third party to perform the needed audit and, if an organization desires, go as far as building a data security audit program from scratch all the way through implementation.

External or third-party auditors are not without drawbacks. Unlike internal auditors, the end result is likely to be absent internal bias or blindness due to proximity. However, an external auditor will lack specific organizational knowledge. Even though a third-party auditor has knowledge of your business, he or she is not likely to have specific information about your organizational culture or business operating practices. As an example, different health plans may offer the same products but are not likely to operate in the same fashion or have the same internal culture.

Quality external auditors, like good mechanics, are sometimes difficult to find. There will likely be some variance between auditors even working for the same organization. Generally, standards have been adopted but individuality prevails, similar to challenges involved in searching for any third-party services. However, in this case your organization will be relying on a third party to perform work that is extremely important to make sure the water is safe and the information security holes aren't so large as to sink the proverbial ship.

Another drawback is cost, although this may or may not be an issue since there is also a cost associated with employing a full- or part-time internal auditor. It may be more cost-effective to employ a third party to conduct, for example, quarterly audits than to employ a qualified internal auditor. Also, larger organizations will likely find it necessary to employ an internal auditor and seek the services of an independent third party to catch those things that may be missed and offer stockholders, the community, the government, etc. an unbiased opinion. In the world of corporate America (and government as well), the outsider tends to have greater credibility, whether it is deserved or not.

As noted, one of the advantages of an external auditor is his or her unbiased perspective. A third party generally will not be privy to the politics of the organization, be swayed by internal opinion, or miss faulty processes because of too much familiarity. The third party tends to bring a fresh set of eyes and can assist in filling the gaps not addressed via an internal audit process.

Third parties tend to follow rigorous standards that can be replicated. An internal audit program can be established independently (or with the assistance of a third party) that is just as rigorous, but a third-party auditor is more likely to follow the same standardized approach used throughout the industry. This is beneficial in reducing legal risk through the consistency and industry acceptance of the approach. It is easier to demonstrate appropriate due diligence by pointing to audit standards followed by someone outside an organization, as opposed to one followed by internal staff.

Organizations also are sometimes required to obtain third-party audits for regulatory or contractual reasons, similar to the annual CPA visit. This becomes a cost of doing business and not a choice in the grand scheme of audit program development.

¶153 Program Management

Whether you use an internal auditor, an external auditor, or both, a management process needs to be established to ensure the program is current, followed, and

repeatable and that identified deficiencies are addressed. The appropriate management structure and program operationalization needs to be laid out prior to rolling out the audit program to the organization. This includes defining who will be expected to assume responsibility for ongoing management.

A program is only a good as its currency, enforcement, and management. It is wise to establish a process up-front to address the following:

- Program management responsibility
- Audit criteria review and revision schedule
- Refresher and new employee training process
- Audit process (the detailed procedures) review and revision schedule
- Audit finding follow-up and escalation process
- Individual or day-to-day mini-audit processes and management
- Regulatory/accreditation compliance requirements and continuous review process

¶154 Placement within the Organization

Developing the program, defining the management structure, and assigning appropriate staff is all well-and-good, but it is only as effective as the acceptance and placement of the program within your organization. Senior management support, as noted earlier, is absolutely necessary to ensure the success of any audit program — financial, operational, data security or otherwise. Also, the official placement within an organization's structure often will decide the fate of the program.

To be effective, an audit program needs to be placed fairly high within an organization. If the perceived and actual power of an audit department or individual is not known, understood, and believed in, audit findings will likely find their way to the bottom of in-boxes and recycle bins. For example, if the program is formed under an accounting department, it is not likely to be as successful as a program operated out of the office of the CEO.

There are mixed opinions about placing a data security audit program under the office of the CIO, which is viewed by some as having the fox guard the hen house. Information technology departments control vast amounts of data, manage networks, control data access, etc. Sometimes organizations will find that those managing the networks may be less likely to see security holes, because they are too close or unwilling to disclose their own network management deficiencies. There is the opposing view that, because the CIO is

closer to the data and highly placed in most organizations, he or she is in a better position to note deficiencies in business processes and see risks more easily than someone not familiar with the technical side of data management.

An alternate approach to placing audit program and audit functions under an individual in the organization is the formation of a data security committee or council, which is made up of senior managers from across the organization. This may provide a more unbiased approach when examining risks, processes, etc. It also sends a clear message that data security management is important to the organization. All of the components of an audit program do not necessarily need to report though one individual or department, even in larger organizations. With the appropriate checks and balances in place, the integrity of an audit program is increased and everyone is "kept honest." ➢➢

¶160 An Audit within an Audit (or Specific versus General Audits)

Once your general audit program has been established and operationalized, it is time to look at specific areas that may present risks to the organization, where specialized audits are needed. Network management, systems development, etc. are areas where more frequent audits are needed. These audits are not the general audit referenced earlier in this chapter but are steps in appropriate systems management.

Data security is not something that can be appropriately managed if it is taken in "too large a chunk." A general audit is needed to document overarching risks and make certain they are being mitigated or managed, processes are followed, etc. Specific and more frequent audit processes should be part of the systems development cycle, part of quality network management, etc.

As an example, a number of organizations run applications and manage IT operations using a Microsoft Windows NT backbone or server base. A sample Windows NT audit process is included below. Similar processes need to be developed to address proper applications development management, security program day-to-day operations, computer data center operations, and other related processes. These become the foundation for solid ongoing data security management.

¶161 Windows NT 4.0 Audit Checklist

A number of steps need to be taken to secure an NT server to minimizing vulnerabilities present in an "out-of-the-box" Windows NT system. Some of those vulnerabilities and how to audit the system against the vulnerability is listed below.

The model audit described utilizes best practices to identify some of the known Windows NT vulnerabilities. The audit helps enforce best practices at the server or network level just as the general audit helps enforce best practices at an organizational level. As with the general audit, an organization needs to determine how secure a network or NT platform needs to be to balance risk against business needs. If rules become too stringent, business operations are impaired while only minimally mitigating risks to an organization.

The SANS web site include an audit criteria checklist. The checklist is not all-inclusive but serves as a brief example of what can be termed an application or process specific audit. As noted, such audits are critical in day-to-day operations to ensure adherence to sound business/data security practices and ongoing protection of an organization's assets. For more complete information about establishing a thorough Windows NT network audit process, visit the SANS Web site at http://www.sans.org and review Chris Young's April 4, 2001 article on the subject entitled, "Windows NT 4.0 Audit Checklist."

¶170 The Need for a Solid Foundation

An effective, quality audit program is based on a solid foundation tailored to fit an organization's business, cultural, and regulatory needs. A number of standard audit program templates exist that can add value when building a program or improving an existing program. Even with such standardized programs, however, it is wise to take a step back and assess whether boilerplate criteria and processes are appropriate "out of the box" or whether they need to be modified to suit an organization's individual characteristics. Determining organizational needs starts with an operational and legal risk assessment followed by a gap analysis. It is imperative that you understand not only "what you do for a living" but how well you are doing the job.

Policies, procedures, and training programs need to be thorough, complete, and well communicated. A well documented data security policy, for example, needs to be operationalized before you move forward with an audit program. An audit program should be designed to measure how well an organization enforces appropriate policies, follows established supporting processes, and communicates all of this to its employees, consultants, and others with whom the organization interacts. Without this foundation, an audit program likely will not be successful in accomplishing the end goal of protecting an organization's

information assets.

Audit programs need to be scalable. An audit program for a small organization will not reach the complexity or cost of one developed for a large multi-state operation. This is part of the tailoring process. An audit program need not be expensive or complex to be effective. It merely needs to be tailored to suit the needs of the organization.

One of the other key factors in the success of a data security audit program is senior management buy-in and organizational understanding. Managers and staff alike need to know that this is a top-down supported program and need to know the "whys" — why time should be spent reviewing processes for security, why time should be spent addressing audit findings, etc. They also need to understand how the program will operate within the organization and what their responsibilities will be in relation to the program.

Even if an audit program is built on a solid foundation and is well-designed, it is likely to fail if it is not appropriately placed within the organization and if ongoing management processes are not established. This holds true for internal, external, or hybrid programs. There is no set formula for how an audit should be conducted or where it should be placed in the organization. Instead, the audit needs to suit the well-defined needs of the organization, remain current in the ever-changing environment of health care, and retain sufficient power to match your responsibilities to "get the job done." HIPAA defines requirements in a very general fashion. It is up to individual organizations not only to create an appropriate process but also to ensure that it works in the long run, because HIPAA is not going away.