



Managing Information Privacy & Security in Healthcare

Privacy and Security Principles

By Ted Cooper, M.D.

From ancient times the importance of privacy has been recognized as essential to patient-physician relationships as stated in the Hippocratic Oath.

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about."¹

High quality health care requires individuals to share sensitive, personal information with their doctors and other health care professionals. This information is necessary to make the most accurate diagnoses and provide the best treatment. This information may be shared with others, such as insurance companies, pharmacies, researchers, and employers, for many reasons. If patients are not confident that this information will be kept confidential, they will not be forthcoming and reveal accurate and complete information. If healthcare providers are not confident that the organization that is responsible for the healthcare record will keep it confidential they will limit what they put in to the record. Either of these actions is likely to result in inferior healthcare. The privacy and security of personal health information has become a major public concern.

The importance and legal justification of privacy is stated in *The Right to Privacy* by Samuel D. Warren, and Louis D. Brandeis in 1890.² The importance of privacy in health care only became a prominent concern in the 1970s. One of the first efforts in this area was initiated by 1972 Elliot Richardson as the Secretary of the US Department of Health, Education and Welfare. This resulted in the publication of a *Code of Fair Information Practices* based on five principles.³

1. There must be no personal data record-keeping systems whose very existence is secret;
2. There must be a way for an individual to find out what information is in his or her file and how the information is being used;
3. There must be a way for an individual to correct information in his or her records;

¹ [Hippocratic Oath – Classic Version](#)

² [Harvard Law Review December 15, 1890](#)

³ US Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii (1973).

4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
5. There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

The principles that support the privacy of healthcare information have since been studied by a great number of initiatives that have all reached similar conclusions, including:

[US Department of Health Education and Welfare 1973 Task Force on the Impact of Computerization of Medical Records Privacy](#)

[Australian Privacy Principles under the Privacy Act 1988](#)

[European Union International Safe Harbor Privacy Principles 1999](#)

Connecting for Health published the results of their efforts in April 2006. They identified nine principles:⁴

1. Openness and Transparency

There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.

2. Purpose Specification and Minimization

The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.

3. Collection Limitation

Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.

4. Use Limitation

Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.

Individual Participation and Control

Individuals should control access to their personal information:

- Individuals should be able to obtain from each entity that controls personal health data, information about

whether or not the entity has data relating to them.

5. Individuals should have the right to:

- Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;
- Be given reasons if a request (as described above) is denied, and to be able to challenge such denial; and
- Challenge data relating to them and have it rectified, completed, or amended.

⁴ [An Overview of the Connecting for Health Common Framework](#)

6. Data Integrity and Quality

All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.

7. Security Safeguards and Controls

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.

8. Accountability and Oversight

Entities in control of personal health data must be held accountable for implementing these information practices.

9. Remedies

Legal and financial remedies must exist to address any security breaches or privacy violations.

Once shared with a health care provider, our personal health information is no longer private and falls subject to various legal and ethical considerations for use and disclosure such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The discipline of information security helps protect shared personal health information. Security has three components: confidentiality, integrity, and availability. The practice of information security requires an ongoing set of activities continually identifying and evaluating threats and vulnerabilities and developing, implementing and monitoring measures to address these threats and vulnerabilities. It must be emphasized that security requires ongoing processes. A one-time check list of security measures to be implemented is likely to be out-of-date and inadequate in a few months. The 1992 OEDC Guidelines for the Security of Information Systems served as the basis for the *Generally Accepted Principles and Practices for Securing Information Technology Systems*⁵ published in 1996 by the National Institute of Standards and Technology which listed eight principles of computer security.

1. Computer Security Supports the Mission of the Organization

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake -- they are put in place to protect important assets and support the overall organizational mission. Security, therefore, is a means to an end and not an end in itself. For example, in a private sector business, having good security is usually secondary to the need to make a profit. Security, then, *ought to* increase the firm's ability to make a profit. In a public-sector agency, security is usually secondary to the agency's providing services to citizens. Security, then, *ought to* help improve the service provided to the citizen.

To act on this, managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission.

⁵ [Generally Accepted Principles and Practices for Securing Information Technology Systems](#)

The roles and functions of a system may not be restricted to a single organization. In an interorganizational system, each organization benefits from securing the system. For example, for electronic commerce to be successful, each participant requires security controls to protect their resources. However, good security on the buyer's system also benefits the seller; the buyer's system is less likely to be used for fraud or to be unavailable or otherwise negatively affect the seller. (The reverse is also true.)

2. Computer Security is an Integral Element of Sound Management

Information and IT systems are often critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees. However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what level of risk they are willing to accept, taking into account the cost of security controls. As with other resources, the management of information and computers may transcend organizational boundaries. When an organization's information and IT systems are linked with external systems, management's responsibilities extend beyond the organization. This requires that management (1) know what general level or type of security is employed on the external system(s) or (2) seek assurance that the external system provides adequate security for their organization's needs.

3. Computer Security Should Be Cost-Effective

The costs and benefits of security should be carefully examined *in both monetary and non-monetary terms* to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IT system. In general, security is a smart business practice. By investing in security measures, an organization can reduce the frequency and severity of computer security-related losses. For example, an organization may estimate that it is experiencing significant losses per year in inventory through fraudulent manipulation of its IT system. Security measures, such as an improved access control system, may significantly reduce the loss. Moreover, a sound security program can thwart hackers and reduce the frequency of viruses. Elimination of these kinds of threats can reduce unfavorable publicity as well as increase morale and productivity. Security benefits do have both direct and indirect costs. Direct costs include purchasing, installing, and administering security measures, such as access control software or fire suppression systems. Additionally, security measures can sometimes affect system performance, employee morale, or retraining requirements. All of these have to be considered in addition to the basic cost of the control itself. In many cases, these additional costs may well exceed the initial cost of the control (as is often seen, for example, in the costs of administering an access control package). Solutions to security problems should not be chosen if they cost more, in monetary or non monetary terms, directly or indirectly, than simply tolerating the problem.

4. Systems Owners Have Security Responsibilities Outside Their Own Organizations

If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be *confident* that the system is adequately secure. This does not imply that all systems must meet

any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security. In addition to sharing information about security, organization managers "should act in a timely, coordinated manner to prevent and to respond to breaches of security" to help prevent damage to others. However, taking such action should *not* jeopardize the security of systems.

5 Computer Security Responsibilities and Accountability Should Be Made Explicit

The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit. The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries. Depending on the size of the organization, the computer security program may be large or small, even a collateral duty of another management official. However, even small organizations can prepare a document that states organization policy and makes explicit computer security responsibilities. This element does *not* specify that individual accountability must be provided for on all systems. For example, many information dissemination systems do not require user identification or use other technical means of user identification and, therefore, cannot hold users accountable.

6. Computer Security Requires a Comprehensive and Integrated Approach

Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

To work effectively, security controls often depend upon the proper functioning of other controls. Many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another. For example, without proper training on how and when to use a virus-detection package, the user may apply the package incorrectly and, therefore, ineffectively. As a result, the user may mistakenly believe that if their system has been checked once, that it will always be virus-free and may inadvertently spread a virus. In reality, these interdependencies are usually more complicated and difficult to ascertain.

The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. Computer security needs to work with traditional security disciplines including physical and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Managers should recognize how computer security relates to other areas of systems and organizational management.

7. Computer Security Should Be Periodically Reassessed

Computers and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connection to external networks; a change in the value or use of information; or the emergence of a new threat. In addition, security is *never* perfect when a system is implemented. System users and operators discover new ways to intentionally or unintentionally bypass or subvert

security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare and procedures become outdated over time. These issues make it necessary to reassess periodically the security of IT systems.

8. Computer Security is Constrained by Societal Factors

The ability of security to support the mission of an organization may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on an IT system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.)

Although privacy is an extremely important societal issue, it is not the only one. The flow of information, especially between a government and its citizens, is another situation where security may need to be modified to support a societal goal. In addition, some authentication measures may be considered invasive in some environments and cultures.

Security measures should be selected and implemented with a recognition of the rights and legitimate interests of others. This may involve balancing the security needs of information owners and users with societal goals. However, rules and expectations change with regard to the appropriate use of security controls. These changes may either increase or decrease security.

The relationship between security and societal norms is not necessarily antagonistic. Security can enhance the access and flow of data and information by providing more accurate and reliable information and greater availability of systems. Security can also increase the privacy afforded to an individual or help achieve other goals set by society.

When implementing a privacy and security program within an organization it is useful to reflect on the principles for privacy and security that have been identified by these efforts.