

**BACKGROUND PAPER – REGULATION  
OF THE SECURITY OF ELECTRONIC  
HEALTH RECORDS**

**David M. W. Young  
Partner, Lang Michener LLP**

**with the assistance of Fern Karsh,  
student-at-law**

**Presented to Shared Risks, Shared Standards Conference  
Toronto, October 23, 2007**

On behalf of my co-chairs – Jeff Curtis of Sunnybrook Health Sciences Centre and Dr. Gordon Atherley of Greyhead Associates – we welcome everyone and thank you for committing a day out of your busy schedules to attend and discuss the important and timely issue of security of electronic health records and electronic health systems.

The title of the conference – “Shared Risks, Shared Standards” – reflects our perception that the security issue is not one that is either “owned” or borne by any one stakeholder group – whether it be government, institutions, providers, professionals or patients. Our perspective is that all stakeholders to some degree do – or should – share the potential risks - and the benefits - and therefore have a shared interest in developing standards.

We are very gratified by the diversity and high calibre of the attendees here today – which we believe validates our perception that the issue *is* one of shared responsibilities – and risks. As we set out in the conference brochure, the real objective of today’s meeting is to try to reach a consensus for a way forward to address the security issue for electronic health records (EHR) systems. Our view is that without clear, and mandated – or at least universally accepted - standards for addressing security, the wide adoption of electronic records and systems within the health sector will be put at risk or at least delayed well beyond the targets that have been set.

While this is the perspective of the conference co-chairs, our objective in organizing this meeting was to seek a consensus among a wide group of stakeholders as to how to move this issue forward. We recognize that the sense of the meeting may either agree with this perspective or it may have a different perspective. However, we do believe that we have an opportunity today not only to discuss what approach should be taken and to articulate the elements of such

approach, but also potentially, to develop a set of outcomes which can be put forward to governments and other policy stakeholders.

To provide a background and context for today's discussion, I shall provide an overview of the current legal framework relevant to the security of electronic health records in Ontario. For comparative purposes I also include references to rules in other jurisdictions. While this overview focuses on the Ontario landscape, many of the principles and certain of the legal rules either apply in other jurisdictions or have parallels there.

By way of clarification at the outset, I should explain that "standards" can mean different things, depending on the context. For the purposes of this conference we mean rules – not necessarily, but potentially, legislative – that govern the users of EHR systems in a way that they will be subject to legal consequences if they fail to comply with them.

In seeking to identify the existing framework for security of EHR systems, we must have reference to the two basic precepts of *confidentiality* and *privacy*. Within the health sector, these are the key existing rules from which the security obligations emanate. Confidentiality and privacy are often treated interchangeably; however they are different, although overlapping, rules.

Confidentiality is an obligation imposed on health professionals and providers – including institutions – to protect and not to disclose patients' or clients' personal health information (PHI) except as expressly permitted. It is an obligation of the health provider. For doctors, the rule emanates initially from their Hippocratic Oath but is now found in their professional codes of practice as well as in legislation such as the *Medicine Act*. For other professionals such as nurses, physiotherapists and pharmacists, the confidentiality rule is found

in their professional codes of practice and in applicable legislation such as the *Nursing Act* and the *Regulated Health Professions Act*. Institutions such as hospitals and social agencies are subject to confidentiality obligations contained in the *Public Hospitals Act*, the *Long-Term Care Act* and other similar legislation.

Typical of these confidentiality rules is the prohibition contained in the *Hospital Management Regulations* under the *Public Hospitals Act*, which reads as follows:

Except as required by law or as provided in this section, no board shall permit any person to remove, inspect or receive information from medical records or from notes, charts and other materials relating to patient care.

Typical of the rules found in professional codes of practice is that found in the Canadian Nurses Association *Code of Ethics* which states:

Nurses must protect the confidentiality of all information gained in the context of the professional relationship, and practice within relevant laws governing privacy and confidentiality of personal health information.

As you can see, these are prohibitions against unauthorized disclosure of PHI; however, they do not directly address security.

Clearly, confidentiality implies security; but security *rules* and *standards* constitute a distinct category: essentially they are the means by which confidentiality is to be achieved. Therefore, while the confidentiality obligation exists for health providers, it contains no explicit directions or rules that address security, or guidance as to the standard of care that can be expected. The obligation does impose potential liability on providers if it is breached however, which creates an incentive for providers to adopt appropriate security measures.

The other key precept from which security criteria emanate is the privacy law. Privacy is distinct from confidentiality because it derives from the *right* of individuals *to control* their personal information, in contrast with the obligation of providers, which is to keep PHI confidential. However, maintaining confidentiality is an aspect of protecting privacy – so the two precepts overlap.

Privacy implies security because one of the principles of a privacy regime – such as is contained in the Canadian Standards Association’s *Model Code for the Protection of Personal Information* (“CSA Model Code”) – is that an individual has the right to have any of his or her personal information that is held by a data collector protected from unauthorized disclosure. The privacy precept therefore is more specific than the confidentiality precept in that it expressly articulates a security requirement.

This security requirement is set out expressly in the privacy laws and it is these laws that form the primary mandate to health care providers to establish appropriate security systems with respect to PHI both generally and, potentially, specifically with respect to electronic health records and systems. It is worth emphasizing therefore that the primary source of statutory direction for security of PHI constitutes the privacy laws. A question to consider in the context of this conference is whether the privacy laws should continue to be the primary, or exclusive, source of direction for security standards applicable to EHRs.

The significance of stipulating the security requirement under the new privacy laws is important: not only does it set a regulatory standard but it also creates a *civil standard of care*, which means that if practitioners or institutions fail to meet this standard, they may be liable in damages to the individuals whose information has been compromised.

The privacy laws not only articulate a required standard of security but contain, in varying degrees, guidance for data collectors as to the nature of the security systems and procedures that should be adopted. However, the primary security obligations contained in Ontario's *Personal Health Information Protection Act* ("PHIPA") is stated in quite general terms. It requires that a custodian take steps *reasonable in the circumstances* to protect information within its custody or control against theft, loss and unauthorized use or disclosure. The Act contains certain additional specific guidance, addressing protection against unauthorized copying, modification or disposal, secure handling and disposal of records. The Act also provides for regulations prescribing more detailed procedures for records retention procedures, electronic data collection and management and electronic network service providers. To date however, only regulations relating to network service providers have been enacted. There are no regulations respecting records management or electronic data procedures, although such regulations are clearly contemplated by the legislation. This deficiency is particularly relevant to the adoption of EHR systems.

PHIPA's lack of detailed guidance respecting security procedures contrasts with the federal law, the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), which through its adoption of the CSA Model Code provides an outline of the nature of the protections that should be adopted. The PIPEDA rule makes clear that such protections should include physical, organizational and technological measures and provides examples of each of these categories. The PIPEDA rule also stipulates that organizations must ensure that their employees are trained in security procedures. PHIPA's approach also contrasts with the other health privacy laws which follow the particularity stipulated in PIPEDA.

While this specificity of required procedures is not currently found in PHIPA, it is clear that, in order to comply with the legislation, custodians are *expected* to adopt detailed procedures. The only difficulty with this approach is that the law itself does not provide the required guidance. Instead, practitioners and institutions must look to other sources, such as international standards setting bodies, industry associations and other stakeholder organizations.

Why is security such a critical element of a privacy regime?

Firstly, the elemental concept of privacy implies an individual's control over and in effect ownership of his or her personal information. Recognition of this concept dictates that if that information is entrusted to another person, that person must take appropriate precautions to prevent that information from being misused, lost or stolen. Furthermore, implicitly, a privacy regime recognizes that if personal information is misused, an individual may suffer injury - whether it be financial, psychological or physical. The security rule seeks to prevent such injury.

Within the health sector, these and other additional reasons underscore why the security rule and effective compliance measures are important. The unauthorized disclosure of an individual's personal health information can have significant injurious impact – whether it be to the individual's dignity and self-esteem, the perception of his or her place in their family and community, or their workplace status. Clearly, this is the most important reason why personal health information must be protected with secure measures.

However, the nature of potential risks go beyond direct psychological and social impact upon the individual. As you know, *identity theft* has become a major concern today and it is a real concern within the health sector. Furthermore, beyond the specific issue of identity theft, there are concerns for protection of the integrity of the health record itself.

In many commercial organizations and to an increasing extent in large health care entities, privacy and security are identified as distinct reporting responsibilities. While it is recognized that they may overlap in many applications – particularly in the health sector – they can have competing priorities and therefore can potentially be in conflict. This circumstance was recognized by the Ontario Information and Privacy Commissioner’s recent report on Smart Systems for Health Agency which recommended that in that organization privacy and security responsibilities should be separated and furthermore that distinct policies should be adopted for each responsibility.

The single electronic health record is generally defined as: a comprehensive compilation of a person’s lifetime health care history, accessible by health care providers across different health systems and different points (e.g. acute care hospitals, physician offices) through electronic networks. By making instantly available a patient’s complete medical history to all health care providers within a circle of care, EHRs have the potential to improve health care delivery. Accuracy, currency, completeness and availability of health data are considered prerequisites to the effective functioning of the health care system, and are made possible through EHRs. EHRs lower the risk of injury due to medical information errors, and have the potential to advance health care research and cut costs by identifying areas for improvement.

While EHRs offer significant advantages to effective health care, they pose challenges to the security of personal health information. Locks and pass-keys, though potentially sufficient in a paper-based system, are inadequate in an electronic environment. Further, in a computerized environment the detriment made possible in the event of unauthorized access is magnified. Computerized databases of personally identifiable information are more vulnerable than paper-based systems because they may be accessed, changed, viewed, copied, used, disclosed, or

deleted more easily and by many more people than paper-based records. The technological means to secure or render unidentifiable personal health information do exist. The challenge is not to invent the technology but rather to ensure that the law has done all that it can to protect the individual's reasonable expectation of privacy and security of personal health information.

As an important adjunct to EHRs, electronic health networks and related software and hardware systems are being adopted aggressively both within institutions as well as province-wide networks. Examples can be found in Ontario's Continuing Care e-Health program, SSHA and the many local and regional networks that share health information. We will hear this morning and in the afternoon workshops from those in the trenches of some of these networks and learn from them how they are dealing with the security challenges. We need to look no further than the recent Ottawa Hospital case for an example of how easy it can be to subvert security procedures in an electronic network.

A further security challenge that is facing the sector involves the inevitable expansion in the use of mobile and wireless devices to collect, communicate and retain PHI. My eyes were opened last year at a conference that focused exclusively on these systems. I learned that they provide the only realistic means for many existing brick and mortar institutions to adopt an electronic network. This is because to hard-wire the existing facilities for a network retrofit would be prohibitively expensive, so a wireless system is the only option. Apart from this design dictate, mobile systems are clearly the future option of choice in medical care – they enable practitioners to collect and communicate data from remote locations – whether they be the patient's bed in a hospital, or community care clients in their homes, or any work site which does not have hard-wire access.

The potential security risks to information collected and managed through these systems are many but – as I learned at the conference last year – can be addressed through strong protective technology and rigorous procedures.

We recognize therefore that it is under the new privacy laws that security of PHI is addressed. As you are aware, the primary focus of the new privacy laws is PIPEDA. PIPEDA applies to commercial entities (and the commercial activities of other entities) and therefore has certain limitations in scope when dealing with the health sector. Four provinces have adopted specific health-sector privacy legislative (Ontario, Manitoba, Saskatchewan and Alberta). Furthermore, all of these laws address, with greater or lesser specificity, the security requirement. All of the provincial laws except Ontario's mandate health information custodians to address the three categories of safeguards identified in PIPEDA: administrative, physical and technological.

However, only Manitoba has addressed with any specificity electronic security. In that province's Act and regulations, protection respecting unauthorized interception, secure destruction and mobile devices is addressed and user logs and audit trails are required. The rules stipulated are quite general in nature but can be contrasted with the other provincial statutes and PIPEDA which at present contain no rules specifically addressing EHRs and the use of electronic systems by custodians.

As noted above, the confidentiality and privacy precepts involve strict obligations to protect PHI – in other words – to ensure that PHI is collected, used and disclosed in a secure manner. However, as is pointed out in the European Union's recent Working Document on the

processing of PHI within EHRs (March 2007), EHR systems create a new risk scenario which calls for new additional safeguards. The EU paper notes that:

EHR systems provide direct access to a compilation of the existing documentation about the medical treatment of a specific person, from different sources (e.g. hospitals, health care professionals) and throughout a lifetime. Such EHR systems therefore transgress the traditional boundaries of the individual patient's direct relationship with a healthcare professional or institution: The keeping of medical information in an EHR extends beyond the traditional methods of keeping and using medical documentation on patients. On the technical side, multiple access points over an open network like the internet increases possible patient data interception. Maintaining the legal standard of confidentially suitable within a traditional paper record environment may be insufficient to protect the privacy interests of a patient once electronic health records are put online. Fully developed EHR systems thus tend to open up and facilitate access to medical information and sensitive personal data.

EHR systems pose significant challenges in ensuring that only appropriate health professionals gain access to information for legitimate purposes related to the care of the data subject. They make the processing of sensitive personal data more complex with direct implications for the rights of the individuals.

The EU's *Data Protection Directive* is considered one of the strongest statements of privacy rules worldwide and was a key point of reference for most Canadian jurisdictions in drafting their privacy laws. The *Directive* contains a very restrictive regime for the processing of PHI, essentially requiring an obligation of *secrecy*, equivalent to the confidentiality role, and a stipulation that any such processing must be *required* for the specific purpose of providing health-related services. However, the Working Paper concludes that this basic requirement of secrecy (i.e. confidentiality) is no longer fully applicable in an EHR environment since one of the purposes of EHR is to provide access to PHI for treatment purposes to professionals who have not been party to the previous treatment documented in the file. Therefore, the Working Paper concludes that the confidentiality obligation does not provide sufficient protection in an

EHR environment: a new risk scenario calls for additional and possibly new safeguards in order to provide for adequate protection of PHI in the EHR context.

The Working Paper articulates the following key areas as requiring special safeguards within EHR systems in order to guarantee patients' privacy rights:

- (i) a patient's self determination of when and how his or her PHI is used, even if the EHR system is not actively founded on consent, (examples would include a framework of different degrees in which the patient can exercise a preparedness to use the system – e.g. opt-in for highly sensitive data versus opt-out for less sensitive data; and reaffirmation of the “Lock-box” principle).
- (ii) reliable identification and authentication procedures applicable to both patients and health care professionals – so that access controls will be possible, including determining the role in which a professional is seeking access.
- (iii) strong access controls to ensure only those professionals who are currently involved in the care are permitted and if feasible a facility for a patient to prevent access if he or she so chooses;
- (iv) creation of different data modules reflecting differing degrees of sensitivity and therefore requiring different access requirements;
- (v) making access by unauthorized persons virtually impossible and, in this regard, applying whenever possible privacy enhancing technologies;

specifically, the legal framework addressing security measures should ensure that it encompasses:

- reliable and effective ID and authentication and up-to-date registers for checking the authorization of persons requesting access;
  - comprehensive logging of all processing steps especially requests for reading or writing;
  - effective back-up and recovery systems;
  - preventing unauthorized access to or alteration of EHR data at times of transfer or back up (e.g. by encryption);
  - clear and documented training for staff including in particular avoidance of security breaches;
  - a clear distinction of functions and competencies for the categories of persons using the system, as may be applicable for determining liability for failures;
  - regular auditing; and
- (vi) finally, an effective system of sanctions based on civil liability that takes into account the respective roles and expectations placed upon the various categories of persons using the system.

If we accept the premise advanced in the EU Working Document, that EHR systems create a new risk scenario for the protection of PHI, where does Canada and more specifically Ontario, stand today in addressing this risk scenario? As I noted above, PHIPA to date does not contain any rules or guidance that are specifically directed to EHR systems. This position is largely identical to that found in the other health privacy law jurisdictions with the exception of Manitoba which in its Act and Regulations has specified certain limited minimum requirements for EHR systems.

In the absence of legislative guidance, the Ontario Information and Privacy Commissioner has articulated certain criteria through her order-making power and through informal guidelines. Specifically, in Order HO-004 the Commissioner has set out certain criteria to address the security of PHI maintained on portable electronic devices. This order contains a number of recommended administrative procedures; its specific application for portable devices addresses recommended procedures for maintaining and providing access to PHI held on such devices. Essentially, the Order mandates effective encryption of such information and the use of multi-layered access authorization procedures.

In another Order, the Commissioner considered security issues related to wireless video communications. The Commissioner stated the general principle that if wireless systems are to be used, the custodian must ensure compliance with the privacy law, and specifically noted that wireless signals must be protected against unauthorized viewing by third parties. She noted that the best currently available technology is encryption or scrambling of such signals.

In her Order made in connection with the Ottawa Hospital case (noted above) – in which a nurse improperly accessed a patient’s electronic file and used information obtained for unauthorized purposes, the Commissioner reviewed the existing procedures and technologies for authorizing access and identifying improper intrusions and concluded that they reflected current standards. However, she made mention of the fact that more sophisticated systems contemplating role-based, or progressively narrower, access rights, and related technologies, are recognized and available but noted that the hospital’s systems did not incorporate such sophisticated technical features for restricting access.

PHIPA does not provide any specific legislative guidance for the security of EHR systems; however at least one other Ontario statute of relevance does address the issue. The regulations under the *Medicine Act* require that if physicians records are maintained electronically, the system must provide for an audit trail, have reasonable protection against unauthorized access and provide reasonable protection against loss, damage to or inaccessibility of information.

By contrast to the approach embraced to this date by Canadian jurisdictions addressing security of PHI and in particular the EHR, other jurisdictions have been far more proactive and directive. We need look no further than the oft-characterized “laissez-faire” environment of the United States to find comprehensive legislative standards. Attached as an appendix to this paper is an outline of the *Security Rule* under the federal *Health Information and Portability Accountability Act* (or “HIPPA”). The rule, while general in nature, contains many requirements directly applicable to EHR systems such as facility access controls, workstation use and security, and device and media controls. The specific *technology-related* requirements address the following key standards:

- access controls
- audit controls
- integrity of PHI
- authentications
- transmission security

A significant feature of the *HIPPA Rule* is that it expressly provides that appropriate security measures must be both scalable and technology neutral. The rationale is that rules need to be suitable for entities of any size or type and they need to allow for change as security technologies evolve. Just as the size and type of an organization determines what is reasonable and appropriate to meet a set of reasonably foreseeable risks, so do technology changes over time.

The U.S. Food and Drug Administration also has published a regulation (21 CFR 11) that sets out in more detail than the *HIPPA Security Rule* requirements for electronic signatures and electronic systems for health records. The regulation is designed to ensure that information in electronic form submitted to the FDA – for example in connection with an application for drug approval – is equivalent to such information if it had been created by paper-based systems and that such electronic form is trustworthy and reliable. The purposes of the regulation are to ensure the integrity of electronic information and confidentiality; its stipulations include minimum procedural and technological standards that must be followed in order for these purposes to be met. A copy of the regulation is also included as an appendix to this paper.

In the absence of legislated standards, a number of stakeholder organizations in Canada have produced valuable work addressing, in varying degrees of detail, standards for EHR system security. The most comprehensive treatment has been provided by Canada Health Infoway which has published several useful discussions documents including the following:

- *Electronic Health Record Privacy and Security Requirements* (Nov. 30,2004/Feb. 7, 2005)
- *Electronic Health Record Infostructure Privacy and Conceptual Architecture* (June 2005)
- *White Paper on Information Governance of the Interoperable Electronic Health Record* (March 2007).

CHI's *Privacy and Security* document contains a detailed listing and discussion of 87 security requirements for an EHR system. These requirements follow closely the ISO/IEC 17799-1 *Code of Practice for Information Security Management*, which also has been widely adopted by health sector and other organizations as a standard of compliance for information security management. CHI's *White Paper on Governance* addresses the broader issues of responsibility and control of information in an EHR system, many of which are relevant to security under the topic "Technical Safeguards". The paper discusses access controls, auditing, handling of security incidents and privacy breaches, and electronic signatures. CHI's *Conceptual Architecture* report provides a high-level view of ten key components, or "services" that are considered critical to privacy and security in an interoperable EHR system. These include for example, user identity and authentications services, access control services,

encryption services and secure audit services. The report also identifies additional features to be considered including protecting patient's identities and patient control over data.

Other sector stakeholders have generated reference documents or guidelines that seek to address many of the security issues posed by EHR systems. These include:

- College of Physicians and Surgeons of British Columbia, *Data Stewardship Framework* (September 2007).
- COACH: Canada's Health Information Association, *Guidelines for the Protection of Health Information* (2006).
- CMA Discussion Paper, "*Electronic Health Records*" (January 2004).

In providing this background for today's discussions, the question that I pose is the following: should Canada's laws and professional standards reflect a pro-active leadership role in establishing basic principles for EHR security, or should we rely on general legal precepts of security to ultimately generate a set of rules, through a more circuitous process? One of my perspectives on our privacy laws is that they should be instructive and preventative, not reactive. While sanctions for breach of the law are essential to ensure compliance of any regulatory regime, providing guidance for users to avoid pitfalls is preferable to penalizing them for breaches. More, importantly, compliance and breach avoidance protects those who would suffer injury: the individual users of the system.

These are some of the issues that we hope to see discussed at today's conference.

## APPENDIX I

### **About the HIPAA Security Rule**

The Security Rule is a part of the Health Insurance Portability and Accountability Act (HIPAA) - federal legislation passed in August 1996. The purpose of the act is to enable better access to health insurance, reduce fraud and abuse, and lower the overall cost of health care in the United States. The final Security Rule became effective as of April 21, 2003.

#### **Application**

The rule applies to electronic protected health information (EPHI) - - individually identifiable health information (IIHI) in electronic form. The primary objective of the Security Rule is to protect the confidentiality, integrity, and availability of EPHI when it is stored, maintained, or transmitted.

Covered Entities (CEs) must comply with the Security Rule. These are health plans, health care clearinghouses, or health care providers who transmit any EPHI.

#### **Upshot**

CEs must maintain reasonable and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of their EPHI against any reasonably anticipated risks.

#### **Penalties**

Noncompliance subjects CEs to civil and criminal penalties. Civil penalties range from \$100 per violation, to \$25,000 per year for each requirement violated. Criminal penalties range from \$50,000 in fines and one year in prison up to \$250,000 in fines and 10 years in jail.

#### **Principles**

The Security Rule is based on the following principles:

1. Scalability
2. Comprehensiveness
3. Technology Neutral
4. Internal and external
5. Risk analysis

## Structure of the rule

The Security Rule's requirements are organized into three categories: *administrative safeguards*, *physical safeguards*, and *technical safeguards*. These categories contain standards, and two-thirds of those standards have implementation specifications. The standard describes the requirement, and an implementation specification describes how it is to be accomplished. The thirty-six implementation specifications are subdivided into those which are required and those which are addressable. Fourteen of them are required. Required specifications must be implemented. Addressable specifications can be handled in one of two ways:

1. If a specific addressable implementation specification is determined to be reasonable and appropriate, the CE must implement it.
2. If implementing a specific addressable implementation specification is not reasonable and appropriate, a CE must:
  - o Document why it would not be reasonable and appropriate to implement the implementation specification; and
  - o Implement and document the alternative security measure that accomplishes the same purpose.

The Security Rule is based on the idea of flexibility. Covered entities must take into account the following factors when deciding which security strategies to use:

- i) The size, complexity and capabilities of the entity;
- ii) The entity's technical infrastructure, hardware and software security capabilities;
- iii) The costs of the security measures; and
- iv) The probability and criticality of potential risks to EPHI.

## Administrative safeguards

Administrative safeguards require documented policies and procedures for managing day-to-day operations, the conduct and access of workforce members to EPHI, and the selection, development, and use of security controls.

The specific standards of the administrative safeguards are:

1. *Security management process* - Implement policies and procedures to prevent, detect, contain, and correct security violations.
2. *Assigned security responsibility* - Designate an individual with overall responsibility for the security of a CE's EPHI.
3. *Workforce security* - Develop and implement policies, procedures, and processes must be that ensure only properly-authorized workforce members have access to EPHI.
4. *Information access management* - Develop and implement policies, procedures, and processes for authorizing, establishing, and modifying access to EPHI.
5. *Security awareness and training* - Develop and implement a security awareness and training program for a CE's entire workforce.

6. *Security incident procedures* - Develop and implement policies, procedures, and processes must be developed and implemented for reporting, responding to, and managing security incidents.
7. *Contingency plan* - Develop and implement policies, procedures, and processes must be developed and implemented for responding to a disaster or emergency that damages information systems containing EPHI.
8. *Evaluation* - Perform periodic technical and non-technical evaluations that determine the extent to which a CE's security policies, procedures, and processes meet the ongoing requirements of the rule.
9. *Business associate contracts and other arrangements* - When dealing with business associates that create, receive, maintain, or transmit EPHI on the CE's behalf -- develop and implement contracts that ensure the business associate will appropriately safeguard the information.

### **Physical safeguards**

Physical safeguards are meant to protect a CE's electronic information systems and EPHI from unauthorized physical access.

The specific standards are:

1. *Facility access controls* - A requirement to implement policies, procedures, and processes that limit physical access to electronic information systems while providing for authorized access.
2. *Workstation use* – Develop and implement policies and procedures that specify appropriate use of workstations and the characteristics of the physical environment of workstations that can access EPHI.
3. *Workstation security* - Implement physical safeguards for all workstations that can access EPHI.
4. *Device and media controls* - Develop and implement policies, procedures, and processes for the receipt and removal of hardware and electronic media that contain EPHI into, out of and within a CE.

### **Technical safeguards**

These are technology-related requirements.

The specific standards are:

1. *Access control* - Develop and implement policies, procedures, and processes for electronic information systems that contain EPHI to only allow access to persons or software programs that have appropriate access rights.
2. *Audit controls* – Implement mechanisms to record and examine activity in information systems that contain or use EPHI.
3. *Integrity* – Develop and implement policies, procedures, and processes that protect EPHI from improper modification or destruction.

4. *Person or entity authentication* - Develop and implement policies, procedures, and processes that verify persons or entities seeking access to EPHI are who or what they claim to be.
5. *Transmission security* - Develop and implement policies, procedures, and processes that prevent unauthorized access to EPHI being transmitted over an electronic communications network.

## APPENDIX II

U.S. Food and Drug Administration

CENTER FOR DEVICES AND RADIOLOGICAL HEALTH

FDA Home Page | CDRH Home Page | Search | A-Z Index Questions?



[510 \(k\)](#) | [Registration](#) | [Listing](#) | [Adverse Events](#) | [PMA](#) | [Classification](#) | [CLIA](#)  
[CFR Title 21](#) | [Advisory Committees](#) | [Assembler](#) | [Recalls](#) | [Guidance](#) | [Standards](#)

[New Search](#)

[Help](#) | [More About 21CFR](#)

[Code of Federal Regulations]  
[Title 21, Volume 1]  
[Revised as of April 1, 2006]  
[CITE: 21CFR11]

TITLE 21--FOOD AND DRUGS  
CHAPTER I--FOOD AND DRUG ADMINISTRATION  
DEPARTMENT OF HEALTH AND HUMAN SERVICES

SUBCHAPTER A--GENERAL  
PART 11 ELECTRONIC RECORDS; ELECTRONIC  
SIGNATURES

**Subpart A--General Provisions**

Sec. 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

[62 FR 13464, Mar. 20, 1997, as amended at 69 FR 71655, Dec. 9, 2004]

#### Sec. 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

#### Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

#### **Subpart B--Electronic Records**

Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and

controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Sec. 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Sec. 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

- (1) The printed name of the signer;
- (2) The date and time when the signature was executed; and
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Sec. 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

**Subpart C--Electronic Signatures**

Sec. 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Sec. 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

**Authority:** 21 U.S.C. 321-393; 42 U.S.C. 262.

**Source:** 62 FR 13464, Mar. 20, 1997, unless otherwise noted.

Database Updated April 1, 2006