

# COMPUTERIZATION OF MEDICAL RECORDS



**James A. Christopherson, ESQ.**  
100 Park Street  
Traverse City, MI 49684  
(231) 929-0500  
(231) 929-0504 - Fax  
Email: [christopherson@ddc-law.com](mailto:christopherson@ddc-law.com)

## BIOGRAPHICAL STATEMENT

James A. Christopherson of Dingeman, Dancer & Christopherson, PLC, represents physicians, physician practices, healthcare organizations, joint ventures, physician organizations, and ambulatory surgery centers. His practice includes advising clients regarding compliance issues, employment issues, litigation, corporate issues including formation, merger and succession issues, and tax exempt legal issues. He practices in the area of healthcare law, commercial litigation, and alternative dispute resolution. He received his B.A., *magna cum laude*, from Michigan State University, and his J.D. degree, *cum laude*, from Wayne State University School of Law, where he received an American Jurisprudence Award and the Silver Key Certificate. He is a member of the State Bar of Michigan and is admitted to practice before the United States Supreme Court (where he has personally argued), the United States District Courts for the Eastern and Western Districts of Michigan, and the United States Court of Appeals for the Sixth Circuit. He is a member of the American Health Lawyers Association, the Health Care Law Sections of the State Bar of Michigan, and the American Bar Association and several committees and working groups. He is a frequent author and speaker on healthcare issues. He has authored several law review articles including "Physician / Hospital Joint Ventures in the Wake of St. Davids" (Journal of Health Law, Winter 2004, Volume 37, No.1), "Buyer Beware When Purchasing a Medical Practice" (Michigan Health Law Report, Summer 2002) and "The Captive Medical Malpractice Insurance Company Alternative" (Annals of Health Law, Volume 5, 1998). He can be reached at [christopherson@ddc-law.com](mailto:christopherson@ddc-law.com) or (231) 929-0500.

## **INTRODUCTION**

With the advent of computer technology, the health care industry, like most other industries, has seen an increasing role in the use of computers in connection with the delivery of health care services. In some instances, it is the use of certain technologies to store paper documents in an electronic format. In others, it is a movement towards the use of the electronic medical record, or EMR. The EMR is designed to replace the paper record as the primary record of care. Unlike paper records, an EMR is designed to not only record the care being provided, but also to provide a way for that information to be interactive. For example, it can include reminders about care. Essentially, it can provide a lifetime record of a patient, a record that can be added to, and accessed by, multiple sources. Regardless to the degree, if any, that a provider or facility uses computer technology, it will enjoy a number of advantages over its paper-only counterparts. That same provider or facility, however, will also magnify some problems and see ones that are unique in the context of computerization of records.

### **A. ADVANTAGES / DISADVANTAGES OF COMPUTERIZED RECORDS**

#### **1. ADVANTAGES**

- a. Immediate access to entire patient histories and treatment, thereby increasing continuity of care and efficiency (cradle to grave approach to documenting a patient's medical history).
- b. Identification of the stage of the medical treatment plan for each individual patient.
- c. Prevention of drug abuse / identification of drug seekers.
- d. Increased billing and collection efficiencies thereby increasing collection rates per patient and decreasing costs.
- e. Lowering healthcare costs by streamlining the administrative and paperwork burdens of healthcare provision.
- f. Eliminates the problem of illegible handwriting.
- g. Can provide clinical prompts with respect to treatment.

#### **2. DISADVANTAGES (most relating to privacy)**

- a. Vulnerability to invisible theft and alteration, with a greater amount of records vulnerable because of the ease of access.
- b. Violation of physician / patient confidentiality and / or other federal and state privacy laws.

- c. Over monitoring by government and large organizations, e.g., the "Big Brother" syndrome.
- d. Computer files are only as good as the information logged into them.
- e. Durability / computer virus / computer sabotage.
- f. Computer down time, inaccessibility and confusion, e.g., problems in networking.
- g. Concern that the type of information accessible is not just medical information (could include family history, sexual practices, drug use).
- h. Concern regarding who is responsible for maintaining the integrity and confidentiality of the records.

The overriding concern of computerization of medical records is privacy. Healthcare records contain sensitive personal information, including name, address, social security number, family history, complaints, diagnosis, medical history, body system descriptions, financial information (including insurance carriers), genetic history, laboratory results, blood tests, x-rays and other sensitive historical data. All patients are intensely concerned about the privacy of this information and they will be much less likely to be candid about their medical, social and family history if privacy cannot be assured, thereby possibly depriving healthcare providers of valuable information which may impact the outcome of individual patient care.

Conversely, a central database of information on each patient for diagnosis, treatment and other purposes is equally important. These two competing concerns must be reconciled. Given the current change of the medical system to managed care, the privacy concerns versus central computerization will become all the more poignant.

## **B. OVERVIEW OF THE LAW**

Current status of the law on computerization of medical records tracks with the status of computerization of records in general, e.g., the law is a confusing patchwork of federal and state statutory and common law protections. These protections include or could include one or more of the following:

### **1. FEDERAL COMMON LAW/CONSTITUTIONAL PROTECTION**

The United States Constitution does not have a specific, discrete constitutional right of protection of privacy. However, privacy interests are found in the First, Third, Fourth, Fifth and Ninth amendments as well as

the Fourteenth amendment=s protection of liberty. Moreover, although the United States Supreme Court has recognized several fundamental privacy rights, it has not extended this protection to informational privacy. Although some commentators suggest that a freedom to care for health and person is a liberty interest within the meaning of the Fourteenth amendment, this has not been specifically decided by the courts. Given the continued proliferation of computerization of medical records, the Supreme Court will be faced with demands to expand constitutional privacy protection to the informational privacy area and recognize that individual freedoms and interests can be interfered with by the government as well as other individuals.

2. FEDERAL PRIVACY ACT OF 1974, 5 USCA ' 552a (1988)

This Act grants individuals more control over the personal information collected, stored, and disseminated by the federal government. The Act requires governmental agencies to notify individuals when the information is collected, reasons for its collection, and whether further disclosure is voluntary or mandatory. The Act contains safeguards or individual privacy rights including standards for limits on data collection. One provision allows the subject access to information about himself or herself and the opportunity to correct inaccuracies, although exceptions to this provision also exist. Despite 12 statutory restrictions, the subject must be allowed the opportunity to consent to further uses of his or her information. The Privacy Act applies to all federal facilities including federally-run hospitals and healthcare facilities that maintain medical records pursuant to contracts with federal agencies.

3. SOCIAL SECURITY ACT REGULATIONS, 42 CFR ' 401.101-401.152

These regulations prevent the disclosure of certain Department of Health and Human Services records subject to several exceptions. Other regulations preserve the confidentiality of patient=s and drug and alcohol treatments at federally funded facilities, 42 USC ' 290dd-3290ee-3.

4. THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA was enacted August 21, 1996 as PL 104-191 and is codified in scattered sections of 42 USC. Its purposes include improving portability and continuity of health insurance coverage, combating fraud and abuse, promoting medical savings accounts, improving access to long-term services and administrative simplification (see <http://aspe.hhs.gov/admsimp/nprm/>).

## 5. STATE STATUTES

The existence of state privacy legislation is also sporadic. Some states have privacy acts and FOIA-like statutes as well as legislation aimed directly at confidentiality of medical information. These statutes vary in quality of protection, and many are not well defined. Privacy protection also is incorporated into medical and professional practice acts and hospital licensure laws.

The gaps in state privacy protection legislation are significant. Little or no protection exists specifically for computer-based information because current laws continue to reflect a paper-based record system. Many state laws require maintenance of records in writing, presumably affording confidentiality and privacy protection solely to such records. Insurance companies are arguably the largest private brokers of healthcare information outside the healthcare field. However, there is very little regulation of insurer disclosure of personal health information. In fact, only a handful of states have adopted model privacy legislation as drafted by the National Association of Insurance Commissioners.

Another shortcoming of state laws is that privacy protection is disease-specific such as the case in Michigan. Although most states have laws protecting human immunodeficiency virus (HIV) and acquired immune deficiency syndromes (AIDS) status from disclosure, disclosure exceptions render actual privacy protection almost nonexistent. Other diseases are protected in varying degrees. Sexually transmitted disease information has strong state protection while tuberculosis and other communicable diseases have little specific legislative privacy protection due to strong public interest in disclosure for public health reasons.

## 6. STATE COMMON LAW

Traditional law causes of action such as invasion of privacy, defamation, and breach of contract have provided theories of recovery in informational privacy cases.

Invasion of privacy, the most common theory asserted, has four commonly recognized branches: intrusion into one's private life, disclosure of one's private affairs, portrayal of one in a false light, and appropriation of one's likeness for the benefit of another. In order to maintain a claim for invasion of privacy, one must show an unreasonable invasion of one's privacy by another and injury resulting from that invasion. A problem with this rule exists as it relates to healthcare data collection in that the low standard of reasonableness is too easily met. Any legitimate reason for collecting or disseminating this information will be found reasonable. Reasonableness is evaluated from the viewpoint of the majority and the need for the information. This standard of evaluation conflicts with

individual interests in protecting one's privacy. The common law provides inadequate protection for informational privacy. The privacy interest protected by traditional invasion of privacy law is not the same as the privacy interest at issue in the misuse of computerized information. Intrusion upon computerized information is not a direct physical violation. The injury comes not in how the intrusion occurs, but in the subsequent actions involving the misappropriated information. There must be a separate, specific check on dissemination of computerized information about an individual.

Another problem with traditional tort theories is that they do not apply unless personal information is disclosed to the public at large. This is especially true with public disclosure of private facts. In the context of computerized records, however, sufficient damage can occur with unauthorized disclosure and dissemination to even one source. For example, an inaccurate notation regarding a medical condition's existence may preclude the subject from obtaining insurance. The additional tort theory requirements that the information normally be considered private and disclosure must be offensive to a person with ordinary sensibilities<sup>4</sup> are also difficult to apply to computerized information. Highly sensitive information can be combined with information of lesser sensitivity and render the whole block of information less sensitive. The ordinary sensibilities<sup>4</sup> standard is becoming difficult to define as offensive public communication grows even more commonplace.

Defamation and the "false light" branch of invasion of privacy are difficult to apply to informational privacy cases. Neither cause of action is particularly applicable to unauthorized disclosure of computerized information. Defamation addresses intentionally false published or spoken communications that injure one's reputation or good name. Defamation requires disclosure to a large enough population so that the community estimation of the defamed is lowered or third parties no longer associate with him or her. Disclosure of information from computerized records can occur "invisibly" and may be to only one unauthorized recipient. Although the recipient population is not large, the resultant damage can be as great or greater than in the case of a widely published statement.

A "false light" privacy cause of action addresses published falsehoods made knowingly or with reckless disregard for the truth. False light privacy causes of action are generally brought against the media for false reports and usually require a showing of malice. Again, this branch of privacy law does not adequately address the kind of intrusion and injury that occurs with computerization. The unique problem in this situation is that computer records are held by many organizations, including private entities as well as governmental agencies; but such records are not generally distributed to the mass media. The damage from unauthorized

disclosure of computerized information is more specific, personal, and insidious. The subject may not even know of the existence of the computer file, its contents, its purpose, or whether the information has been disseminated further.

Recently, breach of contract theory has found some application in lawsuits concerning medical records confidentiality. Ethical standards concerning confidentiality of patient information in the AMA Code of Ethics and state Medical practice Acts form the basis of a contractual relationship between a physician and patient. According to at least two courts, patient reliance on the ethical standards creates an express warranty. Breach of contract results when the ethical standards are violated. The physician=s unauthorized disclosure of medical information to a third party without the patient=s consent is sufficient for a breach of contract claim. In Michigan, a physician=s unauthorized disclosure of confidential information is treated as a claim for medical malpractice.

The long and short of this patch-work of federal and state laws is that advances and computerization will likely result in federal intervention and adoption of comprehensive legislation governing privacy of computerized information in general and, specifically, protection of the privacy of medical records.

### **C. HIPAA AND ELECTRONIC RECORDS**

The “Security Standards for the Protection of Electronic PHI,” are found at 45 CFR Part 160 and Part 164, Subparts A and C. This rule, commonly known as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Congress passed the Administrative Simplification provisions of HIPAA, among other things, to protect the privacy and security of certain health information, and promote efficiency in the health care industry through the use of standardized electronic transactions.

DHHS has published rules implementing a number of provisions, including:

**Privacy Rule** – The deadline for compliance with privacy requirements that govern the use and disclosure of PHI was April 14, 2003, except for small health plans which had an April 14, 2004 deadline. (PHI,” is defined at 45 CFR § 160.103, which can be found on the OCR website at <http://hhs.gov/ocr/hipaa>.)

**Electronic Transactions and Code Sets Rule** – All covered entities should have been in compliance with the electronic transactions and code sets standard formats as of October 16, 2003.

**National Identifier Requirements for Employers, Providers, and Health Plans** – The Employer Identification Number (“EIN”), issued by the Internal Revenue Service (“IRS”), was selected as the identifier for

employers. Covered entities must use this identifier effective July 30, 2004 (except for small health plans, which have until August 1, 2005). The National Provider Identifier (“NPI”) was adopted as the standard unique identifier for HCPs. The Final Rule became effective May 23, 2005. Providers may apply for NPIs on or after that date. The NPI compliance date for all covered entities, except small health plans, is May 23, 2007; the compliance date for small health plans is May 23, 2008. The health plan identifier rule is expected in the coming years.

**Security Rule** – All covered entities must have been in compliance with the Security Rule no later than April 20, 2005, except small health plans which must comply no later than April 20, 2006. The provisions of the Security Rule apply to electronic PHI (“EPI”).

All HIPAA covered entities must comply with the Security Rule. In general, the standards, requirements, and implementation specifications of HIPAA apply to any provider of medical or other health care services or supplies who transmits any health information in electronic form in connection with a transaction for which DHHS has adopted a standard.

## 1. THREE STEPS TO COMPLIANCE

The new rule on the security of electronic patient records boils down to 3 sets of standards/safeguards that practices will need to implement step-by-step.

### **Administrative safeguards**

- Assess computer systems
- Train staff on procedures
- Prepare for aftermath of hackers or catastrophic events
- Develop contracts for business associates

### **Physical safeguards**

- Set procedures for workstation use and security
- Set procedures for electronic media reuse and disposal

### **Technical safeguards**

- Control staff computer log-in and log-off
- Monitor access of patient information
- Set up computers to authenticate users

## 2. APPLICABILITY

The final Security Rule applies only to EPHI. As such, the Security Rule is more limited in scope than the Privacy Rule, which applies to PHI in any

form. The Security Rule applies to EPHI however it may be transmitted or stored and whether or not it is transmitted in a standard transaction governed by the HIPAA Transactions and Code Set Rule. The Security Rule also makes no distinction between communications of EPHI within a corporate entity and those external to the corporate entity. DHHS lists examples of the types of transmissions of EPHI that are subject to the security requirements, including transactions using any electronic media (including the physical movement of information from one location to another in any removable/transportable electronic storage media), such as Internet (wide-open), Extranet, leased lines, dial-up lines, and private networks. Paper and voice transmissions are not subject to the Rule.

### 3. GENERAL SECURITY STANDARDS

The final Security Rule requires each covered entity to meet the following 4 basic security requirements:

- a. Ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits;
- b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- c. Protect against any reasonably anticipated uses or disclosures of such information that are not otherwise permitted or required by the Privacy Rule; and
- d. Ensure compliance with the Rule by its workforce.

The Rule reflects DHHS' emphasis on providing a flexible approach to achieving compliance. Covered entities may use any security measures that allow them "to reasonably and appropriately implement" the Rule's standards and implementation specifications. In deciding which security measures to use, covered entities may take into account the complexity of their organizations, their technical infrastructure (i.e., hardware and software security capabilities), the likelihood and severity of potential risks to EPHI in their operations, and the costs of implementing security measures.

The final Rule establishes 2 types of implementation specifications – those that are "required" and those that are "addressable." Required implementation specifications are just that – required in order to achieve compliance with the Security Rule. Addressable implementation specifications, however, permit a covered entity to assess whether each specification is a "reasonable and appropriate" safeguard in the context of the covered entity's own environment, which is determined by considering such factors as the size and capabilities of and the potential risks to EPHI in its organization.

If a covered entity determines that any addressable safeguard is reasonable and appropriate, it must implement that specification. If the covered entity determines that an addressable implementation specification is not a reasonable and appropriate answer to its security needs, however, the covered entity must document why the implementation specification would not be reasonable and appropriate and implement any equivalent alternative security measure. In addition, the DHHS commentary advises that, if a covered entity determines that it can meet the standard using some other, completely different security measure (i.e., one that is neither an addressable implementation specification nor an equivalent alternative measure), the covered entity may choose not to implement either the addressable specification or an equivalent alternative. In this case, the Security Rule again requires that the covered entity document the rationale for its decision.

Where a security standard has no implementation specifications, the standard itself serves as an implementation specification.

#### 4. ADMINISTRATIVE SAFEGUARDS

In this section of the final Security Rule, DHHS outlines required administrative standards and their corresponding implementation specifications for protecting EPHI. DHHS considered comments that focused on the need for and burden associated with the internal audit requirements, the sanction policy, and the security awareness training, and concluded that the need for these requirements to provide effective security of EPHI outweighed any additional burden these regulations might create for covered entities. To provide more flexibility for covered entities, however, DHHS made some implementation specifications addressable rather than required, reworded others to give covered entities additional discretion in implementing the specifications in a manner appropriate for the size and nature of their businesses, and eliminated from the final Rule several proposed provisions containing more detailed requirements for security safeguards.

##### a. Security Management Process Requirements

The final Security Rule requires covered entities to prevent, detect, contain and correct security violations. The implementation specifications supporting this standard require covered entities to conduct risk analysis and risk management and to establish a sanction policy. The DHHS commentary explains that covered entities must identify the risks to and vulnerabilities of their EPHI before they can take effective steps to eliminate or minimize those risks. This risk analysis specification does not state how often a covered entity must perform a risk assessment, but it does indicate that, to provide adequate security, the covered entity must keep its

security measures “current.” DHHS specifies that a thorough and accurate risk analysis involves consideration of “all relevant losses” expected from unauthorized uses and disclosures and loss of data integrity if security measures were not in place.

The sanction policy prescribed by the Security Rule requires “appropriate sanctions” against any member of a covered entity’s workforce who fails to comply with the covered entity’s security policies and procedures. Many comments addressed what appeared to be the overly harsh mechanism of the proposed regulations to ensure compliance. Other comments required a list of mitigating circumstances, such as good faith, in applying the sanction policy. In its commentary, DHHS responded that punishment is a customary component of adequate security programs and is necessary for effective compliance. However, the Security Rule permits each covered entity to determine the type and severity of sanctions imposed based on its security policy and the relative severity of the violation.

b. Workforce Security

The final Security Rule requires a covered entity to ensure that members of its workforce have appropriate access to EPHI.

c. Security Awareness and Training

The final Security Rule requires covered entities to provide reasonable and appropriate training for their employees. The elements of a security training program are addressable implementation specifications, so covered entities may design their programs to fit their size, risks and operations.

d. Security Incident Procedures and Contingency Plans

The final Security Rule defines “security incident” as “the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.” The final Rule requires a covered entity to create procedures for dealing with a security incident, which DHHS expects it should be able to identify through its risk assessment and risk management efforts. A covered entity is expected to identify and respond to such incidents and to document their occurrence and their “outcomes.” The Security Rule permits, but does not require, covered entities to report security incidents to outside parties.

e. Miscellaneous Administrative Requirements

Other requirements set out in Administrative Safeguards include the need for each covered entity or covered component of a hybrid entity to appoint one official to be responsible for compliance with the Security Rule. The security official's responsibilities include management and supervision of the use of security measures and the conduct of personnel in relation to the protection of data. The security official and the privacy official required under the Privacy Rule have the same roles with respect to the two Rules, and the same person may fill both positions.

5. PHYSICAL SAFEGUARDS

The Physical Safeguard standards set forth the categories of policies and procedures that a covered entity must implement concerning the control of physical access to EPHI stored on hardware and electronic media.

a. Facility Access Controls

This standard requires covered entities to implement policies and procedures that limit physical access to electronic information systems and to all facilities that contain such systems. It also contains addressable implementation specifications that should be evaluated by the covered entity. These cover the development of procedures for facility access in support of the covered entity's disaster recovery efforts, facility security, controlling and validating access to facilities, and documenting repairs and modifications to a facility's security measures.

b. Workstation Use and Security

The Rule requires a covered entity to implement policies and procedures specifying the proper functions to be performed and the manner in which they are performed at workstations that contain EPHI. It also requires policies and procedures governing the physical location and surroundings of such workstations with the goal of maximizing the security of EPHI. Covered entities must also implement physical safeguards that will restrict access to such workstations only to authorized users.

c. Device and Media Controls

The Security Rule also requires covered entities to implement policies and procedures that control the acquisition, disposal and movement of hardware and electronic media that may contain EPHI. These policies and procedures must provide for the final disposition of hardware and electronic media and the removal of

EPHI from media before reuse or recycling. Covered entities must also address the need for (a) maintaining a record of the movements of hardware and electronic media that contain EPHI and of the person responsible for such movements and (b) creating a retrievable, exact copy of the EPHI before equipment is moved.

## 6. TECHNICAL STANDARDS

One of the goals DHHS sets for the security standards is to be technology-neutral. The final Rule, therefore, does not require the use of any specific technologies. It contains general technical requirements that allow implementation of technologies appropriate to each business depending on its needs, size and complexity and the technologies in place.

The technical standards prescribed by the final Rule address access controls, audit controls, integrity (previously referred to as data authentication), person or entity authentication and transmission security. Most of the security implementation features are classified as addressable implementation specifications.

### a. Access Control

Implementation of unique user identification and emergency access procedures is required. However, the encryption and automatic logoff features introduced by the proposed regulations are set forth in the final Rule as addressable implementation specifications and, therefore, need only be implemented as appropriate.

### b. Audit Control

Audit control mechanisms must be implemented to record and examine system activity. This internal audit trail feature, however, will not satisfy the “accounting” requirement of the Privacy Rule, which applies to certain disclosures outside of the covered entity.

### c. Integrity

This safeguard is an addressable implementation specification that involves corroboration of the fact that the data has not been altered or destroyed.

### d. Person or Entity Authentication

Person or entity authentication is required to confirm the identity of the person or entity that seeks access to the data.

e. Transmission Security

In addition to safeguards for stored data, the Security Rule includes a transmission security safeguard that was significantly revised from the proposed regulations to reflect a much simpler and more direct requirement. Encryption is now an addressable implementation specification.

Certain features listed in the proposed regulations were not included in the final Security Rule, such as alarm capability, audit trail, entity authentication and event reporting, all of which are normally provided by telecommunications providers as part of network management and control. In addition, the Security Rule does not require the “Role-based access” or “User-based access” controls that were previously proposed as mechanisms for obtaining consent for the use and disclosure of health information.

7. ORGANIZATIONAL REQUIREMENTS

The final Security Rule creates standards to protect the security of EPHI included in a covered entity’s interaction with its business associates and to which a health plan sponsor may have access. To maintain consistency with the Privacy Rule, the Security Rule adopts several definitions and concepts set forth in the Privacy Rule, including those of “business associate”, “hybrid entity”, and “affiliated entity”.

A major improvement over the proposed regulations is DHHS’s replacement of the “chain of trust agreement” requirement with the “business associate agreement” requirement in the Privacy Rule. The Security Rule simply requires additional provisions in the business associate agreement designed to confirm the business associate’s commitment to provide security and integrity safeguards for EPHI it handles. The expanded business associate agreement must provide that the business associate will:

- a. implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the covered entity;
- b. ensure that any agent to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- c. report to the covered entity any security incident of which it becomes aware;

- d. authorize termination of the contract by the covered entity if the covered entity determines that the business associate has violated a material term of the contract; and
- e. make its policies and procedures related to the implementation of security safeguards available to the Secretary of DHHS for purposes of determining the covered entity's compliance with the security standards.

As in the Privacy Rule, different requirements apply if the business associate and the covered entity are both governmental entities.

The Security Rule also sets forth organizational requirements for group health plans. Agreements between group health plans and plan sponsors generally must require a plan sponsor to:

- a. implement safeguards to reasonably protect the confidentiality of EPHI that it creates, receives, maintains, or transmits on behalf of the group health plan;
- b. ensure that the adequate separation described in the Privacy Rule is supported by appropriate security measures;
- c. ensure that any agent to whom it provides information agrees to implement security measures to protect the information; and
- d. report to the group health plan any security incident of which it becomes aware.

## 8. POLICIES, PROCEDURES AND DOCUMENTATION

Under the final Security Rule, every HCP must develop, maintain, and implement written policies and procedures regarding the receipt, manipulation, storage, dissemination, transmission, and/or disposal of all EPHI. If an HCP amends its policies and procedures for any reason, it must document its revisions. In addition, an HCP must keep its documentation for 6 years after the date of origin or the effective date, whichever is later, and must make its documentation available to the individuals responsible for maintaining and implementing the particular security procedure. Moreover, an HCP must periodically review its policies and procedures and make any revisions that may be required by environmental or operational changes.

## 9. QUESTIONS AND ANSWERS

- a. **Question:** Does the Security Rule apply to written and oral communications?

**Answer:** No. The Security Rule is specific to EPHI. Thus, it does not apply to such items as paper-to-paper faxes, telephones or voice mail systems.

b. **Question:** Am I required to use an electronic signature?

**Answer:** No. Depending on a covered entity's operations, electronic signatures may be appropriate and reasonable and hence used as part of the implementation of the Security Rule's safeguards.

c. **Question:** Does the Security Rule apply to operations outside of a covered entity's facility?

**Answer:** Yes. For example, if a covered entity has employees that work from home and access EPHI, measures have to be taken to protect the EPHI. This can include such things as passwords, automatic log-on/log-off and other reasonable appropriate safeguards.

d. **Question:** How will I know that I am fully compliant with the Security Rule?

**Answer:** You may not. One of the benefits of the Security Rule is its flexibility. As a result, no one plan or program will fit all covered entities. This flexibility, however, also makes it difficult to determine whether there is compliance, since some of the standards/safeguards lack specific parameters. However, those covered entities that engage in risk analysis and risk management on a regular basis will likely be in compliance with the Security Rule.

e. **Question:** What is the purpose of the Security Rule's physical safeguards?

**Answer:** These are designed to: (1) protect the computer systems used in the generation, storage and transmission of EPHI from physical threats such as acts of terrorism; and (2) ensure that a facility and its system is structured such that only those persons who need access to EPHI have that access.

f. **Question:** Can I send EPHI over the Internet or via e-mail?

**Answer:** Yes. Covered entities, however, must ensure the integrity of the EPHI being transmitted. This includes identifying potential vulnerabilities to the network over which the EPHI is being transmitted, and may include the use of encryption and electronic signatures to address those vulnerabilities.

g. **Question:** Does the Security Rule require encryption?

**Answer:** No. As discussed above, it is an addressable specification that may or may not be implemented. Practically, it may be required if it is a reasonable and appropriate safeguard given the covered entity's operations (for example, use of open networks for the transmission of EPHI would likely necessitate encryption unless an equivalent alternative was available).

#### **D. ELECTRONIC RECORDS AND LITIGATION**

As electronic records increasingly form the core of information that is relied upon by practices and facilities, the inherent complexity and malleability of electronic records means that the trustworthiness of them can be challenged. Some of the factors that can undermine the trustworthiness of electronic records include:

1. What is the record? For paper, the record typically exists within the four corners of the document itself. On the other hand, electronic records can consist of data located on different devices in different locations.
2. How trustworthy are such records? Electronic records may be relatively easy to alter or destroy without detection. In contrast, the physical qualities of ink make alteration of paper records more easy to detect.
3. Will the technology be there? Electronic records can only be viewed using computer hardware and software. The necessary technology may not be there in the future. In contrast, paper records can be viewed without the aid of technology.
4. Will courts/juries understand the processes that generated the records? Electronic records may be the result of complex technological processes that are difficult for juries to understand. Since the records must be shown to be trustworthy, it may consume more time and expense demonstrating that such records are trustworthy.
5. What is the chain of custody? Electronic records are more easily created, shared, published and distributed than paper records, making it difficult to keep track of an electronic record during its lifespan. A failure to reliably track the chronology of who had custody and control of an electronic record can diminish its overall trustworthiness.
6. Will the storage devices still work? While paper can easily be used to maintain records over many decades, even over centuries in the right conditions, digital storage mediums have short life spans by comparison. For example, CD's can degrade over time, and may have a shorter shelf life than expected. The threat of technology obsolescence, data corruption, and destruction are greater for electronic records. Also, unlike

paper, which can maintain value as a record even if damaged, electronic records often can be rendered entirely unreadable.

7. Is there too much access? An electronic record's ease of access is also a liability, as vast numbers of records can be stolen or destroyed with just a few key strokes. Such theft or destruction is less likely with paper records.

If you have any questions about the issues raised in these materials, please contact Mr. Christopherson at [christopherson@ddc-law.com](mailto:christopherson@ddc-law.com) or 231-929-0500.

*The opinions expressed in these materials are intended for general guidance only. They are not intended as recommendations for specific situations. The laws, rules, regulations and statutes are subject to change. As always, please consult a qualified attorney for specific legal guidance.*

S:\JAC\CD\INTERNET\2009 Webpage Articles\computerization of medical records.doc