LEGAL ISSUES
IN UTILIZING AND MAINTAINING
COMPUTERIZED MEDICAL RECORDS
IN TEXAS

Corpus Christi, Texas
September 7, 2000

Craig D. Henderson
Gary, Thomasson, Hall & Marks
Professional Corporation
210 S. Carancahua, Suite 500
Corpus Christi, Texas 78401
(361) 884-1961

CRAIG D. HENDERSON is a member of the law firm of Gary, Thomasson, Hall & Marks Professional Corporation, Corpus Christi, Texas. His practice focuses in products liability; general litigation and health law. Born Dayton, Ohio, November 1, 1965; admitted to bar, 1992, Texas; 1993, U.S. District Court, Southern, Western and Eastern Districts of Texas and U.S. Court of Appeals, Fifth Circuit. Education: University of Texas (B.A. in English, 1988); University of Houston (J.D., 1992). Member: Corpus Christi Bar Association; State Bar of Texas; Bar Association of the Fifth Federal Circuit.

This article was prepared to provide general information on the seminar topic presented. It is provided with the understanding that the author is not rendering any legal or professional services. This article is not a substitute for legal advice. Any application of the information contained herein to particular facts or circumstances should be made by legal counsel.

Copyright September 2000
# TABLE OF CONTENTS

I. Advent and Use of Computerized Medical Records ........................................ 1

II. Benefits and Risks of Computerized Medical Records ................................. 4
    A. Benefits .................................................. 4
    B. Risks ..................................................... 4

III. Legal Issues Concerning Computerized Medical Records ............................ 6
    A. HIPAA ...................................................... 6
    B. Liability Resulting from Poor Security or Computer-Use Policies ........ 12
    C. Conclusion ................................................ 14
I. Advent and Use of Computerized Medical Records

The healthcare industry has embraced the use of computer technology and communications networks, including the Internet, in providing services to patients, and both the private and public sectors continue to invest heavily in evolving technologies. The shift from paper records to electronic media for the storage, transmission and processing of medical information, including patient medical records, raises new concerns and challenges for healthcare providers, insurers, managed care organizations, and other groups involved in the delivery of healthcare services, such as protecting patient privacy and insuring that patient medical information is not misused. Because of the immense power of computers to store, organize, analyze and communicate data rapidly, the potential for the misuse of confidential patient information is great and potentially threatens to lessen patient trust in the physician-patient relationship.

In 1991 the Institute of Medicine published its study on computer-based record (CPR) systems, which concluded that computer systems were a necessary component for an evolving healthcare system and called the creation and implementation of computerized patient record systems a priority. A CPR system has been defined as:

[A]n electronic database and communications network that contains each patient's administrative and medical information and that allows clinicians to access the information, schedule tests, and other medical procedures, and communicate across the network with other personnel or departments.
With the increased use of computer based records keeping, the explosion of the internet and internet related transactions, and increased patient nervousness regarding the privacy of their medical information, the government passed the Health Insurance and Portability and Accountability Act of 1996 (“HIPAA”) to, in part, address concerns raised by the evolving technologies in the healthcare industry.

HIPAA is a federal statute which covers a gamut of areas. Its primary purpose is to insure that patients are allowed to maintain health insurance when changing jobs, effectively reduce Medicare fraud and abuse, and simplify the administration of health plans. Of particular interest for the scope of this paper are the rules governing the security and confidentiality of electronic health data and patient information that HIPAA promulgates.

Under the provisions of HIPPA, the Secretary of Health and Human Services was required to issue health privacy regulations by February 21, 2000, given that Congress failed to pass legislation by August 21, 1999. The Secretary has issued proposed regulations. The security and privacy regulations will only become effective 26 months after the proposed regulations become final regulation. The current time frame for the finalization of these regulations is January 1, 2001. Other regulations pertaining to transactional codes have already been approved by the Secretary of Health and Human Services.
But the regulations may only be an interim measure, as Congress has the power following the August 2000 recess to pass legislation that would preempt the regulations and many members of Congress have indicated that that is exactly what they intend to do. Lobbying is intense by diverse groups that fall all across the political spectrum. And the White House is very active in attempting to push its version of legislation through Congress. Concerning computerized medical records, President Clinton said the following in his January 19, 1999, State of the Union address:

As more of our medical records are stored electronically, the threats to all of our privacy increase. Because Congress has given me the authority to act if it does not do so by August, one way or another, we can all say to the American people we will protect the privacy of medical records and we will do it this year.

It therefore appears that the coming months will see significant federal action implementing some form of health privacy protection and regulation of the use and maintenance of computerized medical records. A key issue will be whether the regulations (or possible subsequent legislation) that appears will establish a federal “floor,” setting a minimum level of protection the preempts weaker state laws, but above which states can pass stricter privacy protections if they choose, or establish a federal “ceiling,” thereby limiting the states to pass privacy laws that are no more restrictive than those passed by Congress. Either way, the potential exists for significant changes at both the federal and state levels on health privacy protection.

As the healthcare industry, at all levels, continues to increase utilization of and become dependent upon information technology, the crucial issue raised by this
process will be whether public policy will keep pace with technological use and development.

II. Benefits and Risks of Computerized Medical Records

A. Benefits

There are many benefits that accompany the use of computerized medical records, including the following:

1. Improved quality of medical records;
2. Improved access to and storage of medical records;
3. Improved ability to communicate and deliver medical records to other healthcare providers and insurers;
4. Improved quality of medical care for the patient;
5. Improved ability to analyze treatment and care information for the betterment of patient care;
6. Improved legibility of medical records;
7. Competitive advantage;
8. Expeditious billing and reimbursement processing;
9. Administrative efficiency and reduced costs for maintenance, storage, interpretation, use and communication of medical records; and
10. Improved efficiencies in an integrated healthcare system

B. Risks

The risks associated with the use of computerized medical records include the following:
1. Loss of medical records due to system failures, computer viruses and other causes (e.g., the Y2K problem);

2. Increased difficulty in controlling access to medical records to only authorized personnel;

3. Ease with which medical records can be copied, communicated and disseminated by unauthorized users or by authorized users for improper purposes;

4. Loss of confidence by patients that their medical records will remain confidential and will not be viewed or the information used improperly;

5. Patient fears that computerized medical records in the hands of healthcare insurers, managed care organizations, or the government will be misused to deny benefits, limit coverage or otherwise adversely affect their access to medical services;

6. Erosion of the physician-patient relationship due to patient fears that information conveyed to the physician may be misused;

7. Marginalization of the physician’s role in the healthcare delivery system as insurers, managed care companies, and the government can utilize computerized medical records to influence treatment decisions at the point of service;

8. Decreased quality of care as insurers, managed care companies, and the government could use computerized medical records to reduce the quality of care delivered to patients for reasons of cost-containment;

9. “Corporatization” of medical care; and

10. Increased government regulatory burdens and costs to oversee and enforce the proper use of computerized medical records

The advent and use of information technology has without question brought improvements to both the quality of care delivered by, and access to, the healthcare delivery system; but the opportunity for misuse of computerized medical records is
real and continues to grow as use of computer technology grows. Healthcare privacy
issues in this new information age will continue to be at the forefront of public debate
for many years to come.

III. Legal Issues Concerning Computerized Medical Records

Computerized medical records and their maintenance and use by healthcare
providers, insurers, and managed care entities are subject to the same federal and
state laws as paper records. Because this article is being presented along with other
materials that specifically address those laws, including confidentiality and privacy
issues, alteration or destruction of records, and the duty to provide copies of or
disclose medical records under certain circumstances, this paper focuses on the
specific challenges presented by computerized medical records in complying with
such laws without setting forth the laws in detail.

A. HIPAA

1. To Whom does HIPAA Apply?

HIPAA quite simply applies to all health plans; health care clearing houses
and health care providers who transmit any health information in an electronic form.
The good news is that if you run a completely paper office, then these new
regulations will not apply. The bad news is that virtually no office is computer free.
Accordingly, these regulations will apply to virtually all health care providers.

2. What does HIPAA Protect?
HIPAA seeks to protect the security and privacy of patients’ health information. Health information means any information, whether oral or recorded that is created by a healthcare entity and relates to the past, present or future physical or mental health of a patient. Included is any information pertaining to payments for healthcare. HIPAA applies to any health information that is individually identifiable, that is, or has been, electronically transmitted\(^1\) or electronically maintained\(^2\) by a covered entity, and includes such information in any form. For example, if information is e-mailed and then a paper copy is made of the record, HIPAA will apply to the paper record as well.

HIPAA will require all covered entities with information to use national transaction formats and data content for nine electronic transactions.\(^3\) The rules will also require entities to develop and implement administrative, technical and physical safeguards to ensure the security, integrity, availability and confidentiality of electronic health data. As previously noted, HIPAA is a reaching legislation which will potentially effect large parts of physician practices. We will only be discussing issues pertaining to the maintenance of patients’ health information on computers.

\(^1\) “electronically transmitted” includes information exchange with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmissions over the internet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and “fax back” systems.

\(^2\) “electronically maintained” means information stored by computer or on any electronic medium from which information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, compact disk optical media.

\(^3\) These standards have already been promulgated and approved by the Secretary.
3. Security Regulations

The proposed regulations for security and electronic signature standards consist of a four tiered system to provide adequate security for electronically stored health information. 63 F.R. 43242. While the proposed security regulations have not yet been adopted, it is believed that the final regulations will be issued early in 2001. It is generally thought that there will not be significant changes to the current proposed regulations. Accordingly, this will provide a good precursor for what to expect.

The security regulations create a four tiered approach to provider security to computerized medical records. These regulations range from employee training programs and policies to encryption of medical information.

! Administrative Procedure - Procedure to document what practices and procedures will be put in place to protect data and manage the conduct of personnel in the protection of such data. These procedures include:

-- Certification. - Certify that the appropriate security resources have been implemented. May be performed internally or by accrediting agency.

-- Chain of Trust Partner Agreements. - Contract with third-parties who may process protected data by agreeing that all data transmitted electronically must be secure.

-- Contingency Plans. - Plan to respond to system emergencies including data back-up plans, disaster recovery plans, emergency mode of operation and testing and revision procedures.

-- Record Processing Mechanisms. - Documented policies and procedures for the receipt, manipulation, storage, dissemination, transmission and/or disposal of health information.
-- **Information Access Control.**- Documented policies for granting different levels of access to health care information.

-- **Internal Audits.**- Ongoing internal audits consisting of review of records of system activity (file access, logins, security incidents)

-- **Personnel Security.**- All personnel with access to healthcare information must have authorization after receiving appropriate clearances. Must supervise personnel performing technical systems maintenance, maintaining authorization records, employee personnel clearance procedures.

-- **Security Configuration Management.**- Procedures and practices to ensure system integrity to ensure changes to system hardware/software do not create system weaknesses.

-- **Security Incident Procedures.**- Accurate and current security incident procedures, including reporting response procedures

-- **Security Management Processes.**- Creating policies to ensure the prevention, detection, containment and correction of security breeches. Risk analysis, risk management, sanction policy, security policy.

-- **Termination Procedures.**- Procedures for firing employees to ensure that security of system is not breached, i.e. changing combination lock, removal from access lists, removal from accounts, return of keys, tokens or process cards.

-- **Training.**- Training of personnel including awareness training, security reminders, virus education, password management.

! **Physical Safeguards.**- The physical safeguards to protect the health information consist of:

-- **Assignment of Security Responsibility.**- Assign security responsibility to an individual or organization. Management and supervision of security measures, conduct of personnel in relation to protected data.
-- **Media Controls.**- Formal policies pertaining to the receipt and removal of hardware/software, such as diskettes from the facility. Implementation features including controlled access to media, accountability, data back-up and storage, disposal.

-- **Physical Access Controls.**- Limiting physical access to computer systems by unauthorized individuals. Control such as facility security, plans, procedure to verify access maintenance of records, need to know procedures for personnel access.

-- **Policy/Guidelines on Workstation Use.**- Policy clearly delineating proper use of work stations.

-- **Secure Workstation Location.**

-- **Security Awareness Training.**- Train personnel in security responsibilities.

---

**Technical Security Services.** - The following services are to be implemented in order to protect data integrity, confidentiality and availability:

-- **Access Controls.**- Controls to restrict access to information only to employees who have need to know it. Encryption is optional.

-- **Audit Controls.** - Audit procedures in order to identify suspect access and activities.

-- **Authorization Controls.** - Role based access or user based access.

-- **Data Authentication.** - Procedure which provides corroboration that data has not been altered or destroyed. Checkup, double keying message authentication code, digital signature.

-- **Entity Authentication.** - To ensure that individual accessing information is who he says he is. Automatic log off using I.D.s, biometric I.D. system, passive system PIN, telephone call back, physical device for I.D.
Technical Security Mechanisms. - Mechanism to prevent unauthorized access to information over communication network. This would include the use of integrity controls, message authenticity, access controls, encryption.

4. Privacy Regulations

In addition to the security standards discussed above, DHHS has also promulgated regulations pertaining to privacy issues. In the Standards for Privacy of Individually Identifiable Health Information, 64 F.R. 59918, the Department proposed rules “to protect the privacy of individually identifiable health information.” These standards are far reaching and deal generally with the flow of health information and an effort to ensure that the privacy rights of patients are protected. Unlike the security standards previously discussed, the privacy standards have elicited much debate and comments. In fact, over 150,000 comments have been filed with DHHS. It is not clear, therefore, if these regulations will be substantially changed when finally released, sometime in early 2001.

While many of the privacy standards issues go beyond the scope of this paper, there are some issues which necessarily effect the maintenance of medical records. There are several aspects of the privacy rules, which if they are not changed, will significantly impact the maintenance of electronic medical records, specifically, the administrative requirements of the rules that put in place safeguards for accidental or unauthorized access to medical records.

Designation of Privacy Official. - A covered entity must designate a privacy official who is responsible for the development and implementation of privacy policies and procedures of the entity.
Training - All members of the covered entity’s workforce who are likely to obtain access to health information must receive training on the privacy policies and procedures of the entity.

Safeguards - Implement safeguards to protect health information from intentional or accidental disclosure.

Complaints - Implement a procedure to allow individuals to lodge complaints about an entity’s information practices. A record of such complaints should also be kept. Finally, there must be a contact person responsible for receiving such complaints.

Sanctions - Sanctions for employees and business partners who violate the privacy policies.

B. Liability Resulting from Poor Security or Computer-Use Policies

Computers present unique challenges when it comes to insuring that only authorized personnel have access to medical records or other patient information that is subject to confidentiality and right-of-privacy laws and that medical information is not altered or destroyed. Every provider or other entity that deals with medical records information should have a written computer-use policy that includes policies and procedures to ensure that only personnel who are authorized to deal with medical records information have access to such information and that such information is not improperly altered or destroyed. There are many ways this can be accomplished, and the methods employed depend on the type of computer environment that exists, the purpose and use the computers and other information systems perform, and how the medical records information is used. Qualified computer specialists are well-versed in implementing security protocols to help ensure that only authorized personnel have access to confidential information, and network administrators or service providers
should be tasked with routinely monitoring and insuring the integrity of computer-use security. Typical security measures include passwords, data encryption, an access control list, data-dependent access control, and so-called “firewalls” to protect a network from being infiltrated via the Internet or other communications systems that run to the outside world. Also, all software or data downloaded to a computer or network file server, whether from an internal source of from the Internet or other external source, should be checked for viruses, which have the capability of wreaking havoc with both data and software programs. The use of the Internet for e-mail communication and other purposes has greatly increased the opportunity for malicious computer viruses to be introduced into computer systems. Again, computer specialists should be consulted on how to best deal with this problem.

Those persons who are authorized to access medical records or other confidential information should be instructed to maintain such information as confidential, except to the extent necessary and proper to carry out the providing of healthcare services to the patients involved, and on their duties and obligations to maintain the integrity of said records and, when necessary, produce copies of said records when properly requested. Medical personnel should be aware of, in addition to applicable state and federal laws and regulations concerning maintenance and use of medical records, the applicable provisions of the Code of Medical Ethics of the American Medical Association governing medical records and the use, maintenance and disclosure of medical records information. Authorized personnel should receive
periodic training and education on both computer-use policy and their obligations under the law as to maintaining and using medical records.

Liability for a breach of privacy, unauthorized use, destruction, or alteration of medical records or information contained therein depends upon the particular facts and circumstances of each case and the statutes, regulations or protected rights that were violated. Some statutes and regulations provide specific damage provisions for violations, while other causes of action, such as violation of protected privacy rights, depend upon the nature and extent to which the patient suffered harm, which in some cases could be quite significant (as in the improper or erroneous disclosure of a patient’s HIV status).

Further, HIPAA provides for civil and criminal penalties for the unauthorized disclosure of patient health information ranging from as little as $100 per violation to a $250,000 fine or 10 years in prison for the knowing and wrongful disclosure of a patient’s health information with bad intent. Clearly, patients’ privacy rights in their medical records which are stored on computers are being taken very seriously by DHHS and the government as a whole.

C. Conclusion

Although the HIPAA regulations will not be in effect for at least two years, the scope and breadth of these requirements will likely require significant time and resources to implement. Some experts have estimated that the cost associated with the implementation of HIPAA will exceed the costs associated with the Y2K problem. The HIPAA requirements should be considered before making any
software and hardware purchases. HIPAA requires that “[a]ny standard adopted...shall be consistent with the objective of reducing administrative costs of providing and paying for health care.” 42 USCA §1320d-1(d). It is yet to be seen how these regulations will reduce costs in the long run. It is clear, however, that in the short run the implementation of HIPAA will be expensive, technically difficult, and time consuming.