MEDICAL RECORDS LAW IN MICHIGAN

JAMES A. CHRISTOPHERSON, ESQ.
100 Park Street
Traverse City, MI 49684
(231) 929-0500
(231) 929-0504 - Fax
Email: christopherson@ddc-law.com
BIOGRAPHICAL STATEMENT

James A. Christopherson of Dingeman, Dancer & Christopherson, PLC represents physicians, healthcare organizations, physician organizations and ambulatory surgery centers. His practice includes advising clients regarding compliance issues, employment issues, corporate issues including formation 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 and former president of the Grand Traverse-Leelanau-Antrim Bar Association. 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).
TABLE OF CONTENTS

I. INTRODUCTION ............................................................................................................................................. 1

II. SUMMARY OF LAW RELATING TO CONFIDENTIALITY OF MEDICAL RECORDS ................................................................. 1

   A. MEDICAL ETHICS ............................................................................................................................................. 1
       1. Hippocratic Oath ........................................................................................................................................... 1
       2. American Medical Association ...................................................................................................................... 1

   B. STATE OF MICHIGAN STATUTES, RULES AND REGULATIONS ......................................................................... 2
       1. Physician/Patient Privilege ............................................................................................................................ 2
       2. Clinical Patient Records (Health Maintenance Organizations) ..................................................................... 2
       3. Physician=s Assistant Privilege ...................................................................................................................... 2
       4. Third Party Administrators ........................................................................................................................... 3
       5. Health Care Facilities or Agencies .............................................................................................................. 3

   C. FEDERAL STATUTES, RULES AND REGULATIONS .................................................................................. 5
       1. Medicare Requirements ................................................................................................................................. 5
       2. Health Maintenance Organizations .............................................................................................................. 5
       3. Drug Abuse Records ..................................................................................................................................... 5

   D. ACCREDITING ORGANIZATIONS .............................................................................................................. 6
       1. National Committee for Quality Assurance (NCQA®) ..................................................................................... 6
       2. Joint Commission on Accreditation of Health Care Organizations (JCAHO®) .................................................. 6
       3. Accreditation Association for Ambulatory Health Care .............................................................................. 6

   E. COMMON EXCEPTIONS ................................................................................................................................... 7

III. MICHIGAN’S MEDICAL RECORDS ACCESS ACT .................................................................................. 7

IV. OVERVIEW OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) ...................................................... 10

   A. GENERAL OVERVIEW OF HIPAA REQUIREMENTS .................................................................................. 10
       1. Goal Of HIPAA ............................................................................................................................................. 10
       2. Compliance Deadline .................................................................................................................................... 10
       3. Abbreviations and Definitions ...................................................................................................................... 10
       4. HIPAA Security Rules .................................................................................................................................. 12
           a. Boundaries ................................................................................................................................................. 12
           b. Security ..................................................................................................................................................... 12
           c. Consumer Control .................................................................................................................................... 12
           d. Accountability .......................................................................................................................................... 12
           e. Public Responsibility ............................................................................................................................... 12
B. HIPAA COMPLIANCE ................................................................................................................................. 13
1. What If I Don’t Comply? ........................................................................................................................ 13
2. General Penalties for Failure to Comply ................................................................. 13
3. Who Can Sue?................................................................................................................................. 13

C. EVOLUTION OF THE CURRENT STATUS OF HIPAA REGULATIONS ................. 14
1. The August 14, 2002 Final Regulations ............................................................................... 14
2. Incidental Uses and Disclosures ......................................................................................... 15
3. Minimum Necessary Standard ......................................................................................... 16
4. Personal Representatives ........................................................................................................ 16
5. Business Associates ........................................................................................................ 16

D. USES AND DISCLOSURES FOR TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS .................................................................................................................. 17

E. NOTICE OF PRIVACY PRACTICES FOR PHI ......................................................... 18

F. STEPS TO HIPAA COMPLIANCE................................................................................................. 19

G. FEBRUARY 16, 2006 FINAL HIPAA ENFORCEMENT RULE ......... 20

H. JUSTICE DEPARTMENT JUNE 9, 2005 MEMORANDUM ................ 21

I. HIPAA QUIZ ........................................................................................................................................... 22

J. CASE STUDY ............................................................................................................................................... 26
1. United States v Gibson ............................................................................................................... 26
2. University of Colorado v Denver Publishing ........................................................................ 27

V. RETENTION OF MEDICAL RECORDS ................................................................................. 27

A. MICHIGAN MEDICAL RECORDS RETENTION ACT ........................................ 27

B. MEDICAL RECORDS: HEALTH FACILITIES GENERALLY .................. 28

C. AMERICAN MEDICAL ASSOCIATION, 1994 CODE OF MEDICAL ETHICS, 7.05(2) ................................................................................................................................. 28

D. MEDICARE HOSPITAL MANUAL, CHAPTER 3 – ADMISSION PROCEDURES 301.3 ................................................................................................................................. 29

E. JCAHO 2000 ACCREDITATION MANUAL FOR HOSPITALS, IM.6.1 .... 29

F. MENTAL HEALTH SERVICES ................................................................................................. 29

G. HOME HEALTH AGENCY ........................................................................................................ 30
H. HOSPICE ............................................................................................................. 30
I. LONG TERM CARE FACILITY ........................................................................ 30
J. HIPAA ............................................................................................................... 30
   1. Notice of Privacy Practices ....................................................................... 30
   2. Policies and Procedures .......................................................................... 31
   3. Consent Forms .......................................................................................... 31
   4. Authorizations ......................................................................................... 31

VI. UNDERSTANDING AND NEGOTIATING EMR LICENSING AGREEMENTS ... 31

VII. ADVANCE DIRECTIVES AND ACCESS TO MEDICAL RECORDS ............. 33
   A. WHAT IS AN ADVANCE DIRECTIVE? ..................................................... 33
   B. THE DURABLE POWER OF ATTORNEY FOR HEALTH CARE IN MICHIGAN ........................................................................................................... 33
      1. Incapacity of patient ........................................................................... 36
      2. Binding Effect ..................................................................................... 36
      3. Petition to Probate Court .................................................................. 37
      4. Pregnancy ............................................................................................ 37
      5. Limitation on Health Care Provider .................................................. 37
      6. Limitations on Life and Health Insurance Companies ........................ 37

VIII. ALTERATION AND DESTRUCTION OF MEDICAL RECORDS ............... 37
   A. OWNERSHIP OF MEDICAL RECORDS ................................................. 38
   B. ALTERATION OF PATIENT RECORDS UNDER MICHIGAN LAW ......... 38
      1. General Rules ...................................................................................... 38
   C. UETA AND E-SIGN .................................................................................. 40
      1. UETA .................................................................................................... 40
      2. E-SIGN ................................................................................................. 40

IX. PRIVILEGE/CONFIDENTIALITY ................................................................... 43
   A. GENERAL RULE ...................................................................................... 43
   B. EXCEPTIONS/NUANCES ........................................................................ 43
   C. ADMINISTRATIVE PENALTIES ............................................................ 43
   D. COMMON LAW CAUSES OF ACTION .................................................. 44
      1. Invasion of privacy ............................................................................... 44
2. Breach of fiduciary duty ................................................. 44
3. Breach of contract - express or implied ................................ 44
4. Negligence .................................................................. 45
5. Defamation .................................................................. 46
6. Negligent Infliction of Emotional Distress ...................... 46
7. Intentional Infliction of Emotional Distress ...................... 47
8. Breach of Duty to Disclose ............................................ 47
10. ERISA - Preemption and Liability ................................. 48

X. HIPAA – STATE LAW PREEMPTION AND SUMMARY OF HIPAA AND STATE LAW DIFFERENCES .............................................. 48

   A. GENERAL RULE .................................................................. 48
   B. EXCEPTIONS .................................................................. 48
   C. SPECIFIC EXAMPLES .......................................................... 49

XI. MICHIGAN AIDS LEGISLATION .................................................. 53

   A. CONSENT AND HIV TEST COUNSELING ....................... 53
   B. REPORTING REQUIREMENTS ........................................... 54
   C. PARTNER NOTIFICATION .................................................... 54
   D. CONFIDENTIALITY REQUIREMENTS .............................. 55
   E. MARRIAGE APPLICANTS .................................................... 55
   F. PREGNANCY ................................................................ 56
   G. MINOR’S CONSENT TO TREATMENT FOR HIV ............... 56
   H. BLOOD AND ORGAN DONATIONS .................................... 56
   I. ARTIFICIAL INSEMINATION ............................................. 57
   J. EMERGENCY CARE ............................................................ 57

XII. SUBPOENAS ........................................................................ 57

   A. INTRODUCTION ................................................................ 57
## B. REQUIREMENTS OF A SUBPOENA .................................................. 60
1. Subpoena Requesting Production of Medical Records .......... 60
2. Subpoena Requesting Appearance or Production of Records at ......
   Trial (MCR 2.506) ........................................................................ 61
3. Service of Subpoena (MCR 2.105, MCR 2.506(G)) .............. 61
4. Compliance with Subpoena ......................................................... 61

## XIII. ELECTRONIC TRANSMISSION AND SECURITY STANDARDS .............. 62

A. OVERVIEW .................................................................................. 62

B. THREE STEPS TO COMPLIANCE .................................................. 63

C. APPLICABILITY ............................................................................ 63

D. GENERAL SECURITY STANDARDS ................................................. 64

E. ADMINISTRATIVE SAFEGUARDS ..................................................... 65
   2. Workforce Security ................................................................. 66
   3. Security Awareness and Training ..................................... 66
   4. Security Incident Procedures and Contingency Plans ......... 66
   5. Miscellaneous Administrative Requirements ................. 66

F. PHYSICAL SAFEGUARDS ................................................................. 67
   1. Facility Access Controls .......................................................... 67
   2. Workstation Use and Security ............................................... 67
   3. Device and Media Controls ..................................................... 67

G. TECHNICAL STANDARDS ................................................................. 68
   1. Access Control ....................................................................... 68
   2. Audit Control ........................................................................... 68
   3. Integrity ..................................................................................... 68
   4. Person or Entity Authentication ............................................ 68
   5. Transmission Security ............................................................ 68

H. ORGANIZATIONAL REQUIREMENTS .............................................. 69

I. POLICIES, PROCEDURES AND DOCUMENTATION ............................. 70

J. QUESTIONS AND ANSWERS ........................................................... 70

## XIV. COMPUTERIZATION OF MEDICAL RECORDS AND SECURITY ISSUES ...... 73

A. ADVANTAGES / DISADVANTAGES OF COMPUTERIZED RECORDS . 73
   1. Advantages ............................................................................. 73
   2. Disadvantages (most relating to privacy) ......................... 74
B. CURRENT STATUS OF LAW ................................................................. 75
   1. Federal Common Law/Constitutional Protection ......................... 75
   4. The Health Insurance Portability and Accountability Act (HIPAA) . 76
   5. State Statutes ............................................................................. 76
   6. State Common Law .................................................................... 77

XV. MEDICAL RECORDS AND LITIGATION ............................................ 79
   A. IMPORTANCE OF MAINTAINING GOOD/COMPLETE MEDICAL
      RECORDS ..................................................................................... 79
   B. PHYSICIAN/PATIENT PRIVILEGE .................................................. 79
      1. Statutory - MCLA '600.2157 ..................................................... 79
      2. Exceptions ............................................................................... 79
   C. PSYCHOLOGIST AND PSYCHIATRIST/PATIENT PRIVILEGE ......... 80
      1. Statutory - MCLA '330.1750 ..................................................... 80
      2. Exceptions ............................................................................... 80
   D. SUBSEQUENT TREATING PHYSICIANS ......................................... 81
      1. Production of records ................................................................ 81
      2. Testimony in court / at deposition ............................................. 81
      3. Interviews by attorneys ............................................................ 81
   E. MISSING RECORDS ...................................................................... 82
   F. WHAT RECORDS MUST BE PRODUCED ....................................... 82

XVI. MINORS AND INCOMPETENT ADULTS ............................................. 84
   A. IN RE ROSEBUSH ....................................................................... 84
   B. IN RE MARTIN ............................................................................ 85

XVII. PATIENT SELF-DETERMINATION ACT .......................................... 86
   A. WHO MUST COMPLY WITH THIS LAW ........................................ 86
   B. WHAT MUST A HEALTH CARE ENTITY DO? ............................... 86
      1. Written requirements ............................................................... 86
      2. Oral requirements ................................................................... 87
      3. Compliance with state laws ..................................................... 87
      4. Education ............................................................................... 87
I. INTRODUCTION

Information and records about a person’s medical condition have traditionally been held to be confidential. The reason for confidentiality of medical records is to encourage candor in the physician-patient relationship. There are a number of state laws, federal laws and regulations and ethical rules which uphold the confidentiality of information about a person’s medical condition.

II. SUMMARY OF LAW RELATING TO CONFIDENTIALITY OF MEDICAL RECORDS

A. MEDICAL ETHICS

1. Hippocratic Oath

Whatever in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret.

2. American Medical Association

5.05 CONFIDENTIALITY. The information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree. The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services. The patient should be able to make this disclosure with the knowledge that the physician will respect the confidential nature of the communication. The physician should not reveal confidential communications or information without the express consent of the patient, unless required to do so by law.

The obligation to safeguard patient confidences is subject to certain exceptions which are ethically and legally justified because of overriding social considerations. Where a patient threatens to inflict serious bodily harm to another person and there is a reasonable probability that the patient may carry out the threat, the physician should take reasonable precautions for the protection of the intended victim, including notification of law enforcement authorities. Also, communicable diseases, gun shot and knife wounds should be reported as required by applicable statutes or ordinance.

American Medical Association, Current Opinions of the Judicial Counsel of the American Medical Association. 5.05 at 19 (1984).
B. STATE OF MICHIGAN STATUTES, RULES AND REGULATIONS

1. Physician/Patient Privilege

No person duly authorized to practice medicine or surgery shall be allowed to disclose any information which he may have acquired in attending any patient in his professional character, and which information was necessary to enable him to prescribe for such patient as a physician, or to do any act for him as a surgeon; provided, however, that in case such patient shall bring an action against any defendant to recover for any personal injuries, or for any malpractice, if such plaintiff shall produce any physician as a witness in his own behalf, who has treated him for such injury, or for any disease or condition, with reference to which such malpractice is alleged, he shall be deemed to have waived the privilege hereinbefore provided for, as to any or all other physicians, who may have treated him for such injuries, disease or condition; provided further, that after the decease of such patient, in a contest upon the question of admitting the will of such patient to probate, the heirs at law of such patient, whether proponents or contestants of his will, shall be deemed to be personal representatives of such deceased patient for the purpose of waiving the privilege hereinbefore created. MCL 600.2157.

2. Clinical Patient Records (Health Maintenance Organizations)

Information contained in the clinical patient record shall be treated as confidential, shall be disclosed only to authorized persons, and shall be available at all times to the department for purposes of examination and review.

An inactive record shall be safely stored and preserved electronically or as an original record or microfilm. The health maintenance organization shall adopt a policy concerning the length of time and provisions for the retention of inactive clinical records, which shall include a contingency plan for the retention of existing records in the event of cessation of operations. R 325.6810.

3. Physician’s Assistant Privilege

A physician’s assistant is the agent of the supervising physician. A communication made to a physician’s assistant that would be privileged communication if made to the supervising physician is a privileged communication to the physician’s assistant and the supervising physician to the same extent as if the communication were made to the supervising physician. MCL 333.17078.
4. Third Party Administrators

a. A third party administrator (TPA) shall provide for the confidentiality of personal data identifying an individual covered by a plan. A TPA shall not disclose records containing personal information that may be associated with an identifiable individual covered by a plan to a person other than the individual to whom the information pertains. Except as is necessary to comply with a court order, an administrator shall not disclose personal data concerning a covered individual without the prior consent of the covered individual. If the individual covered by a plan has authorized the release of information to a third person, the third person shall not release that information unless the individual executes in writing another consent authorizing the additional release.

b. Subjection (a) shall not be construed to apply to information disclosed for any of the following reasons:

i. Claims adjudication.

ii. Claims verification.

iii. An audit conducted pursuant to ERISA.

iv. To an insurer for the purchase of excess loss insurance and for claims under the excess loss insurance. However, an insurer obtaining information under this subdivision shall be subject to the requirements of subsection (a).

v. To the plan or a fiduciary of the plan.

vi. To the commissioner. However, information obtained by the commissioner under this subdivision shall be exempt from disclosure under the freedom of information act, Act No. 442 of the Public Acts of 1976, being sections 15.231 to 15.246 of the Michigan Compiled Laws. MCL 550.934.

5. Health Care Facilities or Agencies

A patient or resident is entitled to confidential treatment of personal and medical records, and may refuse their release to a person outside the facility except as required because of a transfer to another health care facility or as required by law or third party payment contract.
A patient or resident is entitled to associate and have private communications and consultations with his or her physician, attorney, or any other person of his or her choice and to send and receive personal mail unopened on the same day it is received at the health facility or agency, unless medically contraindicated as documented by the attending physician in the medical record. MCL 333.20201.

6. Mental Health Records

Section 748 of Michigan Public Health Code

(1) Information in the record of a recipient, and other information acquired in the course of providing mental health services to a recipient shall be kept confidential and shall not be open to public inspection.

(4) For case record entries made subsequent to March 28, 1996, information made confidential by this section shall be disclosed to an adult recipient, upon the recipient’s request, if the recipient does not have a guardian and has not been adjudicated legally incompetent.

The holder of the record shall comply with the adult recipient’s request for disclosure as expeditiously as possible but in no event later than the earlier of 30 days after receipt of the request or, if the recipient is receiving treatment from the holder of the record, before the recipient is released from treatment.

(6) Except as otherwise provided in subsection (4), if consent is obtained from the recipient, the recipient’s guardian with authority to consent, the parent with legal custody of a minor recipient, or the court-appointed personal representative or executor of the estate of a deceased recipient, information made confidential by this section may be disclosed to all of the following:

(a) A provider of mental health services to the recipient.

(b) The recipient or his or her guardian or the parent of a minor recipient or another individual or agency unless in the written judgment of the holder the disclosure would be detrimental to the recipient or others.

A parent to whom a court has granted joint legal custody, but not physical custody, of a minor child may consent to the
release of, and have access to, the minor child’s mental health records under section 748(6) of the Mental Health Code, unless in the written judgment of the holder of the records the disclosure would be detrimental to the minor child or others.


C. FEDERAL STATUTES, RULES AND REGULATIONS

1. Medicare Requirements

Federal Medicare requirements provide that information from or copies of records may be released only to authorized individuals, and the hospital must insure that unauthorized individuals cannot gain access to or alter patient records. 42 CFR ‘482.24(b)(3). Hospitals are required to have a procedure to insure for the confidentiality of patient records. Other entities must also maintain confidential records. CFR ‘483.420(a)(7) (long term care facilities), 42 CFR ‘484.48(b) (home health agencies); 42 CFR ‘485.56(c)(5) (comprehensive outpatient rehabilitation facilities) (requires procedures for preparing and maintaining clinical records, but not specifically confidentiality procedures), 42 CFR ‘485.638(b) (rural primary care hospitals); 42 CFR ‘491.10(b) (rural health clinics).

2. Health Maintenance Organizations

If an HMO is federally approved, it must comply with the Federal Health Maintenance Organization Act of 1973, 42 USC ‘300e. This Act requires that as a condition of qualification by the Department of Health and Human Services that the HMO must establish adequate procedures to insure the confidentiality of the health and medical records of its enrollees. 42 CFR ‘417.406(d).

3. Drug Abuse Records

Records of the identity, diagnosis, prognosis, or treatment of any patient which are maintained in connection with the performance of any drug abuse prevention function conducted, regulated, or directly or indirectly assisted by any department or agency of the United States shall, except as provided in subsection (e) of this section [Armed Forces and Veterans Administration interchange of Records], be confidential and be disclosed only for the purposes and under the circumstances expressly authorized under subsection (b) of this section. 42 USC ‘290ee-3.

D. ACCREDITING ORGANIZATIONS

1. National Committee for Quality Assurance (NCQA®).

2. Joint Commission on Accreditation of Health Care Organizations (JCAHO®).

In order to obtain and maintain JCAHO accreditation a hospital or another health care organization must meet JCAHO requirements. The following sections are from the Accreditation Manual for Hospital 1994. The following confidentiality standards should be satisfied by hospitals in order to be assured accreditation. They include:

a. RI.1.1.8 The right of the patient, within the limits of law, to personal privacy and confidentiality of information . . . (emphasis added).

b. IM.2.1 The organization determines the need for and appropriate levels of security and confidentiality of data/information.

c. IM.2.2 The organization determines how data/information can be retrieved on a timely basis without compromising the data's/information's security and confidentiality.

   IM.2.2.1 A written organizational and medical staff policy requires that medical records may be removed from the organization's jurisdiction and safekeeping only in accordance with a court order, subpoena, or statute.

   IM.2.2.2 The organization has a functioning mechanism designed to preserve the confidentiality of data/information identified as sensitive or requiring extraordinary means to preserve patient privacy. (emphasis added)

d. IM.2.3 The organization has a functioning mechanism designed to safeguard records/information against loss, destruction, tampering, and unauthorized access or use.

e. IM.10.3 The information management function maintains the security and confidentiality of data/information when contributing to or using external databases.

f. SO.3.2.3 Confidentiality of Information.

3. Accreditation Association for Ambulatory Health Care
E. COMMON EXCEPTIONS

1. Communications made in furtherance of unlawful or criminal purpose (i.e. testimony of physician relative to alterations in a prescription by patient charged with obtaining a controlled substance by fraud.) People v Lawrence Johnson, 111 Mich App 383 (1981).


4. Communications for the purpose of a lawsuit and not for treatment (i.e. results of blood test taken to disprove paternity.) Osborn v Fabatz, 105 Mich App 450 (1981).

5. Review of records by peer review organizations regarding services for which payment has been made under Title VIII of the Social Security Act.

6. Reports to state and federal agencies gathering health data (i.e. births, deaths, birth defects, AIDS, etc.).

7. Information released to a board or department acting within the scope of its authority regarding the licensure and regulation of health care professionals. MCLA 333.16244.

8. Reports of abuse of nursing home patients to the Department of Health. MCLA 333.21771.

9. Reports of suspected child abuse to the Department of Social Services. MCLA 722.625.

10. Reports of abuse of physically or mentally impaired adults to the Department of Social Services. MCLA 400.11a.

11. In an action for malpractice


13. HIPAA: treatment, payment or operations ("TPO").

III. MICHIGAN’S MEDICAL RECORDS ACCESS ACT
A. Under the MMRAA, “[e]xcept as otherwise provided by law or regulation, a patient or his or her authorized representative has the right to examine or obtain the patient’s medical record.” See Sec. 5(1). If the patient is deceased, an “authorized representative” is defined as “his or her personal representative or his or her heirs at law of the beneficiary of the patient’s life insurance policy, to the extent provided by” MCLA 600.2157. See Sec. 3(a)(ii). MCLA 600.2157 limits access by heirs at law to situations where there is “a contest upon the question of admitting the patient’s will to probate.” It is not clear whether the existence of a personal representative will preclude access by an heir at law, as there is no question that, under current practice, health care providers and other record keepers will not release health-related information to “mere” heirs.

B. Health professionals that are not subject to the MMRAA include those that provide health care solely through the sale or dispensing of drugs or medical devices or a psychiatrist, psychologist, social worker, or professional counselor who provides only mental health services. MCL 333.26263(e).

C. When presented with a request for medical records by a person, a health care provider (“HCP”) cannot inquire about the reason for the request. In order to comply with HIPAA authorization standards that require an authorization to include a description of the purpose, an authorization form could state: “You are not required to tell us the purpose of your request. If you do not wish to tell us, simply check the box that states ‘at my request.’ If you wish to provide more detailed information, you may do so here:”

D. The HCP must respond within either 30 days, if the records are on-site, or 60 days if the records are off-site.

E. The response can take several forms.

1. Records can be made available for inspection or copying.

2. The HCP can contact the medical records company retaining the records to have them made available for inspection or copying.

3. If the records do not exist or cannot be located, the patient must be so advised.

F. An HCP can extend the time to respond by up to 30 days provided it notifies the person in writing. It may not make more than 1 extension per request.

G. Under limited circumstances, the HCP can refuse to provide the records. If disclosure is “likely to have an adverse effect on the patient,” the HCP can notify the patient in writing and have the records provided to a HCP, facility or attorney of the patient’s choosing.
H. If the records were compiled by the HCP under a confidentiality agreement, the HCP can deny the request if the disclosure “would be reasonably likely to reveal the source of the information.”

I. Fees.

1. $20 initial fee per request.
2. $1 per page for the first 20 pages.
3. 50¢ per page for pages 21-50.
4. 20¢ per page for pages 51 and beyond.
5. Postage and shipping costs.
6. Costs incurred in retrieving medical records that are 7 years old and older and not maintained or accessible on site.

J. The HCP can condition compliance on receipt of the applicable fee. Beginning in 2006, the fee shall be adjusted based upon changes in the Detroit consumer price index.

K. If the patient is “medically indigent,” the HCP must waive all fees as to the first set of copies. “Medically indigent” generally includes those persons receiving Social Security benefits or who have applied for medical assistance from the State of Michigan. An HCP cannot charge the medically indigent patient the $20 initial fee.

L. While the title of the Act indicates that it merely addresses the same issues that are already the subject of exhaustive federal and state regulation, its provisions do address an area of uncertainty confronting HCPs. With the passage of the Act, HCPs no longer have to speculate whether the fees they are charging persons requesting medical records are reasonable.

M. Due diligence should be exercised in attempting to locate requested medical records. In the event records are missing, the requesting party should be promptly notified. The alteration or destruction of a medical record by an HCP for purposes of concealing responsibility for a patient’s injury is a felony. MCLA 750.429a.

N. Violation.

1. $1,000 fine.
2. Misdemeanor.
3. Criminal penalties.

O. What Records Must Be Produced.

A commonly asked question among HCPs is what medical records must be produced by the provider. Many providers take the position that only the records generated by that provider need be produced.

Many providers take the position that there was never a release from the other providers who generated the records. The Medical Records Access Act of 2004, however, defines "medical record" very broadly to include:

…information oral or recorded in any form or medium that pertains to a patient’s healthcare, medical history, diagnosis, prognosis, or medical condition and that is maintained by a healthcare provider or health facility in the process of the patient’s health (emphasis added).

With an appropriate authorization seeking “any and all medical records,” it would appear that a physician is required to release the entire stack of records, even those produced by other care providers. Not only is the term “medical records” defined broadly, the language of the patient’s authorization that calls for the release of “any and all medical records” appears broad enough to encompass more than the provider’s own generated records.

P. Section 11: The MMRAA does not apply to copies of medical records provided to third party payers or insurers.

IV. OVERVIEW OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

A. GENERAL OVERVIEW OF HIPAA REQUIREMENTS

1. Goal Of HIPAA

The goal of HIPAA is to improve efficiency and effectiveness of electronic information transfers used in the provision, management and funding of healthcare in the U.S.

2. Compliance Deadline

Final compliance must have occurred by April 14, 2003.

3. Abbreviations and Definitions

Business Associates
A person, other than an employee, who performs a function involving the use of PHI

Covered Entities
Includes health plans, billing companies, healthcare systems and providers who engage in electronic transactions

DHHS
Department of Health and Human Services

E PHI
Electronic Protected Health Information

Guidelines
Guidance on Privacy Standards dated July 6, 2001, issued by the OCR

HCP
Health Care Provider

HIPAA
Health Insurance Portability and Accountability Act of 1996

NPI
National Provider Identifier

Notice of Privacy Practices
Notice of the use and disclosure of PHI that may be made by a Covered Entity and of the individual’s rights and the Covered Entity’s legal duties with respect to PHI

OHCA
Organized Health Care Arrangement

OCR
Office of Civil Rights (within DHHS)

PHI
Protected Health Information

Privacy Rules
December 28, 2000 Standards for Privacy of Individually Identifiable Health Information promulgated by the DHHS as amended on August 14, 2003

Standards
December 3, 2002 Standards for Privacy of Individually Identifiable Health Information

TPO
Treatment, Payment or Health Care Operations
Website
www.hhs.gov/ocr/hipaa

4. HIPAA Security Rules – effective April 21, 2005. HIPAA Rationale:

a. Boundaries

Individual healthcare information should be used for health purposes only, subject to a few carefully defined exceptions. It should be easy to use information for defined purposes and very difficult for other purposes.

b. Security

Federal law should require those to whom we entrust health information to protect it against deliberate or inadvertent misuse or disclosure.

c. Consumer Control

Patients should be able to see what is in their records, get a copy, correct errors, and find out who else has seen them.

d. Accountability

Those who misuse information should be punished, and those who are harmed by its misuse should have legal recourse.

e. Public Responsibility

Privacy must be balanced by public responsibility to contribute to the common good. This includes oversight, public health, research, and law enforcement.
B. HIPAA COMPLIANCE

Large health care systems to individual provider offices must comply with the new regulations. Regardless of the amount or whether your office transmits information electronically, your office must comply with HIPAA.

1. What If I Don't Comply?

The law provides for severe financial and criminal penalties for violations.

2. General Penalties for Failure to Comply

   a. Each violation carries a fine of $100 with a maximum penalty of $25,000 for violations of the identical requirement. Example: Billing clerk transmits nonstandard coding to payer.

   b. Wrongful disclosure of health care data carries a fine of $50,000, imprisonment of not more than 1 year, or both. Example: Disclosure of results to unauthorized individuals.

   c. Release of health care information under false pretences carries a fine of $100,000, imprisonment of not more than 5 years, or both. Example: Providing false information.

   d. Knowingly releasing patient data with the intent to sell information carries a fine of $250,000, imprisonment of not more than 10 years, or both. Example: Selling patient information to a pharmaceutical company.

3. Who Can Sue?

   a. Private parties cannot bring lawsuits against the press under HIPAA. University of Colorado Hospital Authority v Denver Publishing Co, Aug. 2, 2004. If followed by other courts, this decision will diminish one potential source of claims against the media for reporting information related to hospital patients.

   In 2003, an anonymous source mailed to the Rocky Mountain News a copy of a confidential peer-review report of Dr. Issam Awad, a prominent neurosurgeon at the University of Colorado Hospital. The report asserted that Awad provided substandard care in several surgeries and violated ethical standards.

   Although the hospital’s medical board cleared Awad, he resigned and took a position elsewhere. The hospital first
invoked HIPAA when it sued last October to try to stop the newspaper from publishing any information in the report.

A federal judge, however, decided that blocking publication would be an unconstitutional “prior restraint” on the press. After the newspaper published the report as part of a series on Awad and the peer-review process, the hospital again sued under HIPAA, this time seeking monetary damages.

Although the statute is targeted at hospitals and HMOs, the hospital zeroed in on one provision that could be read to apply to anyone – including the press – who discloses medical information.

The newspaper argued that the case should be dismissed because HIPAA does not create a private right of action – meaning that only the government, not a private party, can go to court to enforce the statute.

In what is believed to be the first decision to address the issue of private-party lawsuits against the press under HIPAA, the court agreed. Neither the privacy provisions of HIPAA, however, nor any other section of the statute explicitly create a private right of action, the court found.

Moreover, the privacy provisions specifically establish that the government may seek to impose fines and imprisonment on violators. This leaves no room for an implied private right of action, the court concluded.

C. EVOLUTION OF THE CURRENT STATUS OF HIPAA REGULATIONS

1. The August 14, 2002 Final Regulations

Consent for treatment, payment and health care operations is optional. HCPs must make a “good faith” effort to obtain a written acknowledgment as of the first date of service.

HCPs must provide patients with written notice of their privacy practices and patients' privacy rights.

a. Patients may:
   i. access their personal medical records;
   ii. correct errors contained in those records; and
iii. request a breakdown of the non-routine uses and disclosures of their health information.

2. Incidental Uses and Disclosures

The Privacy Rule permits incidental uses and disclosures of PHI, as long as an HCP applies reasonable safeguards and, where applicable, the minimum necessary standard.

a. Examples of Reasonable Safeguards

i. Using a lowered voice when discussing PHI in public areas

ii. Avoiding use of patient names in public hallways or elevators

iii. Posting signs to remind employees to protect patient confidentiality

iv. Isolating or locking file cabinets or record rooms

v. Limiting non-employee access to areas containing PHI

vi. Placing patient charts facing the wall or covering them to limit the visibility of PHI

vii. Using passwords on computers maintaining PHI

viii. Having patients stand a few feet back from a pharmacist counter used for patient counseling

ix. Using cubicles, dividers, shields, curtains or similar barriers where multiple staff-patient communications occur

x. Limiting PHI disclosed on a patient answering machine or over an intercom system

xi. Not showing the purpose of a physician visit on patient sign-in sheets
3. Minimum Necessary Standard

The Guidance notes that the minimum necessary standard does NOT apply to:

a. Disclosures to or requests by an HCP for treatment purposes
b. Disclosures to the individual who is the subject of the PHI
c. Uses or disclosures based on the individual’s authorization
d. Uses or disclosures required for compliance with HIPAA
e. Disclosures to DHHS when required under HIPAA for enforcement purposes
f. Uses and disclosures required by other law

4. Personal Representatives

The Guidance clarifies when family members may access PHI of other family members:

a. Disclosure of PHI for treatment purposes does not require authorization – even when the disclosure is for the treatment of another individual. An HCP may, therefore, disclose PHI of one family member if necessary for the treatment of another family member.

b. An HCP must treat a deceased individual’s legally authorized executor or administrator as a personal representative with respect to PHI relevant to such representation.

c. The Privacy Rule imposes no specific additional requirements on HCPs for identifying or verifying a personal representative. Since this is a matter for state or other law, HCP should continue to identify such persons as they do now.

5. Business Associates

The Guidance notes that a business associate contract is NOT required in the following situations:

a. When an HCP discloses PHI to a health plan for payment purposes
b. When access to PHI is incidental, such as in connection with janitorial services, and certain contractors, such as electricians, plumbers, or copy machine technicians

c. When a person or entity is acting merely as a messenger for PHI such as the United States Postal Service, private couriers and their electronic equivalents

d. When HCPs participating in an organized health care arrangement (OHCA) make disclosures of PHI that relate to the joint health care activities of the OHCA

e. When PHI is disclosed to a researcher for research purposes based on patient authorization, waiver of authorization, or in the form of a limited data set.

D. USES AND DISCLOSURES FOR TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS

The Privacy Rule does not change informed consent and consent for treatment laws because the Privacy Rule relates to the use and disclosure of PHI and not to consent to treatment.

Michigan law:


1. A hospital may use PHI to:
   a. provide health care;
   b. to consult with another HCP; and
   c. send a patient’s health care instructions to a nursing home to which the patient is transferred.

2. A hospital emergency department may give a patient’s payment information to an ambulance service so that the ambulance service may bill the patient.
3. A primary care doctor may send a patient’s medical record to a specialist who needs the information to treat that patient.

4. HCPs to whom a patient is referred for the first time can use that patient’s PHI to set up appointments and schedule surgery because this use is for treatment, payment or health care operations.

5. An HCP may consult with other providers without a patient’s authorization for treatment purposes.

6. Disclosures for Worker’s Compensation
   
a. The Privacy Rule permits HCPs to disclose PHI to workers’ compensation insurers, state administrators, employers and other persons or entities involved in workers’ compensation systems, in the following circumstances:

   i. To comply with workers’ compensation laws or similar programs established by law that provide benefits for work-related injuries or illness;

   ii. For purposes of obtaining payment for any health care provided to injured or ill workers; and

   iii. As required by state or other law.

   The worker’s compensation or insurance representatives of an employer may have access to the medical records of an employee-patient examined and treated in the medical clinic of the employer for an injury sustained during the employment, but information secured and placed on the medical records by an attending physician or physicians which is not relevant to the claim of the employee-patient for worker’s disability compensation may not be disclosed without the waiver of the employee-patient. Opinion No. 6593 of the Michigan Attorney General, 1989.

E. NOTICE OF PRIVACY PRACTICES FOR PHI

1. Direct treatment providers, other than in emergency situations, must provide the Notice at or before the first service delivery date, and must make a good faith effort to obtain a written acknowledgment.

2. Health plans do not need to obtain a written acknowledgment.

3. When the first treatment encounter is not face-to-face, HCPs may mail the Notice and provide a tear-off sheet to be returned as an acknowledgment.
4. HCPs may distribute their Notice through the mail as part of other mailings.

5. Health plans may distribute the Notice with the distribution of Summary Plan Descriptions.

6. The Notice may not be combined in a single document with an authorization form.

7. Business associates do not need to create a Notice, but their uses and disclosures of PHI must be consistent with those of the HCP.

8. Participating members of an OHCA may rely on a single Notice.

9. If the patient is a minor child, Notice can be given to the parent, guardian, or person acting in *loco parentis*.

10. When changes are made in the Notice, a revised Notice does not need to be mailed or distributed. Rather, the revised Notice must be provided upon request, and posted where the HCP has a physical service delivery site.

F. STEPS TO HIPAA COMPLIANCE

1. Prepare Notice of Privacy Practices/ Acknowledgment (if necessary) and follow it

2. Adjust for state law provisions

3. Replace release forms with authorization forms

4. Train workforce members

5. Set up an individual rights process for your policy on individual rights

6. Forms for access, amendments and accounting

7. Implement policies and procedures to comply with all HIPAA Privacy Standards

8. Develop/update computer access and role based access policies for minimum necessary compliance

9. Tighten storage and destruction of patient information to safeguard PHI
10. Conduct a security walk-through/security standards

11. Comply with Security Rule by April 21, 2005

12. Set up internal mechanisms to track and log disclosures for accounting and amendments

13. Update patient communications for HIPAA compliance

14. Enter into Business Associate Agreements

15. Designate a privacy official

16. Conduct review for miscellaneous HIPAA compliance, e.g. disclosures by (group) health plans to plan sponsor, research requirements, etc.

17. Implement policies and procedures to comply with HIPAA Security Standards

G. FEBRUARY 16, 2006 FINAL HIPAA ENFORCEMENT RULE

The DHHS has published the final HIPAA enforcement rule on February 16, 2006. The proposed rule is available on the OCR website, http://www.hhs.gov/ocr/hipaa/>, by clicking on “Final Enforcement Rule Published.” The Final Rule, which takes effect March 16, 2006, adopts unified enforcement procedures for the Privacy Rule and the other HIPAA Administrative Simplification rules, such as the Security Rule. In addition, the Final Rule establishes procedural and substantive requirements for the imposition of civil money penalties (“CMPS”) for violations of the HIPAA provisions. The adoption of the Final Rule completes the regulatory enforcement structure begun when the Privacy Rule was issued in 2000 and expanded by the interim final procedural enforcement rules issued in 2003. The proposed rule replaces an interim enforcement rule published 2 years ago that primarily covered steps the government would take to impose civil fines for violations of non-privacy HIPAA rules. Many provisions of the interim rule are included in the proposed rule, but the scope of the proposed rule is much larger.

An enforcement regulation written into the privacy rule prohibits intimidation or other retaliatory action against individuals or HCPs that file a non-compliance complaint or cooperate in enforcement processes. Under the enforcement rule, that regulation now protects individuals or entities filing complaints of any HIPAA rule violations.

Under the rule, the Centers for Medicare and Medicaid Services would continue to be responsible for enforcing the non-privacy rules; the Officer for Civil Rights will continue to enforce the privacy rule.
The rule also implies that DHHS may stray from its philosophy of investigating the compliance status of HCPs only upon receipt of a complaint of non-compliance. Compliance and enforcement activities have been primarily complaint-based. DHHS indicates it may also conduct compliance reviews to determine if a covered entity is in compliance.

Under the enforcement rule, the DHHS will maintain its current practice of working with non-compliant HCPs to help them become compliant, reserving civil fines or filing criminal complaints only if an HCP does not cooperate. The rule lays out the enforcement processes DHHS will take. The department will refer violations subject to criminal penalties to the Department of Justice.

The rule indicates that shared liability between an HCP and its business associate is unlikely if the HCP followed all of the requirements of the HIPAA privacy rule. Those requirements mean executed agreements with business associates to safeguard PHI and due diligence to oversee and ensure that protections are carried out.

HCPs in compliance with the business associate provisions of the HIPAA security and privacy rules would not be liable for any violation by the outside entities, even though the business associate is the HCP’s agent and was acting within the scope of its agency when it violated the rule. The rule does not distinguish between an action or an inaction – failure to protect data is viewed as the equivalent of intentionally releasing it.

H. JUSTICE DEPARTMENT JUNE 9, 2005 MEMORANDUM

Under a memo the Justice Department issued on June 9, 2005, HIPAA’s criminal enforcement provision applies directly to “covered entities,” which include physicians and other health professionals specified in the statute, health plans, health care clearinghouses and Medicare prescription drug card sponsors. “In addition,” the memo states, “depending on the facts of a given case, certain directors, officers, and employees of these entities may be directly liable.” But the memo adds, “Other persons may not be directly liable under this provision.”

Under HIPAA, criminal penalties apply to those who “knowingly” misuse other people’s protected health data. In clarifying the meaning of the word “knowingly” in this context, the memo states that it requires proof only that the alleged perpetrator knew of the facts of the offense. It does not require proof the person knew what he or she was doing violated HIPAA.

The Justice Department memo also states that most health care workers – those who are not covered entities – are not criminally liable for the misuse of another person’s PHI, at least not under HIPAA.
I. HIPAA QUIZ

1. To comply with HIPAA regulations, it is required that all entities utilize electronic transmissions of health data.

   *FALSE.* HIPAA does not require electronic transfer of health data, although it does establish privacy and security standards for electronic transfers.

2. I don’t perform my own billing or coding, therefore I am not required or responsible to comply with the HIPAA federal regulations.

   *FALSE.* There should be a Business Partner Agreement in place between the HCP and the firm performing coding and billing. This should hold the coding/billing firm contractually obligated to comply with the regulations.

   **NOTE:** Although this agreement may be in place, it is the provider who is accountable.

3. My practice management software provides an upgrade software package that conforms to HIPAA standards. Upon installation of this upgrade, my practice will meet HIPAA compliance.

   *FALSE.* Although most people feel HIPAA is a technology issue, in reality, HIPAA is 25% technology and 75% business process changes. While upgrading your practice management software may be necessary, there are other aspects of the HIPAA regulations that require compliance.

4. You are not required to receive Business Associate Agreements from pharmaceutical representatives, postal service employees, and courier services.

   *TRUE.* You are not required to receive Business Associate Agreements from service employees who are not intended to receive PHI. These are considered incidental disclosures and are permissible under HIPAA.

5. I don’t submit electronic claims, therefore I am not required or responsible to comply with the HIPAA federal regulations.

   *TRUE.* Entities that do not submit electronic claims are not required to comply with HIPAA. If outside billing partners submit electronic claims on your behalf, your organization is then considered a covered
entity and required to comply with all aspects of HIPAA. Entities may continue to submit non-electronic claims, although electronic submission is less labor intensive, processed quicker, and payments are received faster.

6. **Sign-in sheets are permissible under the new HIPAA regulations.**

   *TRUE.* Sign-in sheets are permissible under the new privacy regulations. It is a recommended practice to request a patient signature and date on sign-in sheets, but no other identifiable information.

7. **My office receptionist and transcriptionist share the same password to access patient files. This practice is acceptable under HIPAA.**

   *FALSE.* Sharing of passwords eliminates any methodology of using them correctly. With HIPAA requirements of audit controls, it would be difficult or impossible to accurately track who was accessing any specific record at a given time when passwords are shared.

8. **Financial penalties can be up to $250,000 for failure to comply with HIPAA guidelines.**

   *TRUE.* Financial penalties for intentionally selling PHI can be up to $250,000 and/or jail time. HIPAA is a serious issue and compliance is mandatory.

9. **PHI is only information contained in electronic form.**

   *FALSE.* The definition of PHI has been expanded to include all individually identifiable health information transmitted or maintained by a covered entity regardless of form. This includes electronic, paper, and verbal means of communication.

10. **You must have your own policies and procedures manual to be compliant with HIPAA.**

    *TRUE.* Policies and procedures must be consistent with the HIPAA requirements.

11. **Must an HCP obtain an individual’s authorization to use or disclose PHI to an interpreter?**

    *No.* Authorization is not required when:
a. the interpreter is a member of the HCP’s workforce (i.e. a bilingual employee, a contract interpreter on staff, or a volunteer) as defined at 45 CFR 160.103; or

b. the HCP hires the services of a person or entity, who is not a workforce member, to perform interpreter services as a business associate, as defined at 45 CFR 160.103.

PHI may be disclosed for business associates (private commercial companies, community-based organizations, or telephone interpreter service lines) to provide interpreter services, subject to certain written assurances set forth in 45 CFR 164.504(e).

HCPs may use and disclose PHI for treatment, payment and health care operations without an individual’s authorization, 45 CFR 164.506(c).

An HCP might use interpreter services to communicate with patients who speak a language other than English or who are deaf or hard of hearing, and provision of interpreter services usually will be a health care operations function of the HCP as defined at 45 CFR 164.501.

An HCP may use or disclose PHI to the patient’s family member, close friend, or any other person identified by the individual as his or her interpreter for a particular healthcare encounter, without the individual’s authorization. In these situations, the interpreter is not a business associate of the HCP.

As with other disclosures to family members, friends or other persons identified by an individual as involved in his or her care, when the individual is present, the HCP may obtain the individual’s agreement or reasonably infer that, based on the exercise of professional judgment, the individual does not object to the disclosure of PHI to the interpreter. 45 CFR 164.510(b)(2).

The Privacy Rule requires the HCP to verify that these conditions are met, as well as the identity and authority of the public official making the request, unless already known to the HCP. The HCP must also limit the disclosures to the minimum necessary for the purpose.

12. **Are you covered against HIPAA lawsuits? Probably not!**

Physicians and providers are usually not protected from civil HIPAA litigation by their standard malpractice, errors and omissions, or general liability policies.

13. **How does an HCP respond to a subpoena?**
An HCP receiving a subpoena should determine whether a request for records constitutes an “order of a court or administrative tribunal” or a subpoena or discovery request, because the standards for HIPAA compliance are significantly different for these two types of requests.

HIPAA allows an HCP to disclose PHI in the course of any judicial or administrative proceeding “in response to an order of a court or administrative tribunal, provided that the Covered Entity discloses only the protected health information expressly authorized by such order.”

An HCP that receives a court order signed by a judge that directs it to release an individual’s medical information, the HCP may do so without patient authorization.

The HCP may disclose only the PHI that is expressly authorized in the court order and not more. If the HCP does not comply with the court order, it risks being held in contempt of court.

The Privacy Rule permits an HCP to disclose PHI “in response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal,” but only if the following requirements are met:

A. The HCP receives satisfactory written assurance from the party seeking the information (the Requestor) that reasonable efforts have been made by the Requestor to ensure that the patient has been given notice of the request.

B. The HCP receives satisfactory written assurance from the Requestor that reasonable efforts have been made by the Requester to secure a qualified protective order.

14. **May a health plan disclose PHI to a state child support enforcement (IV-D) agency in response to a National Medical Support Notice?**

Yes. The Privacy Rule permits disclosure of PHI to a “law enforcement official” for law enforcement purposes in compliance with court orders, grand jury subpoenas, or certain written administrative requests. 45 CFR 164.512(f)(1)(ii).

A “law enforcement official” means an officer or employee of any agency or authority of:

a. the United States,
b. a state,

c. a territory,

d. a political subdivision of a state or territory, or

e. an Indian tribe,

who is empowered by law to investigate or conduct an official inquiry into a potential violation of law or to prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. 45 CFR 164.501. An employee of an IV-D agency, including a contract employee, who is empowered by state or federal law to enforce a medical child support order, meets this definition of a law enforcement official.

The NMSN, a national uniform form which is sent by the IV-D agency to the employee and health plan for completion, constitutes a written administrative request by a law enforcement official.

The Privacy Rule allows disclosure of PHI in response to the NMSN, provided it includes or is accompanied by written assurances that:

a. The information sought is material and relevant to a legitimate law enforcement inquiry;

b. The request is specific and limited in scope; and

c. De-identified information cannot reasonably be used.


J. CASE STUDY

1. United States v Gibson

A Washington state man pled guilty in federal court on August 19, 2004 to wrongful disclosure of a patient’s PHI. This was the first criminal conviction in the United States under HIPAA.

Richard Gibson, an employee at the Seattle Cancer Care Alliance, admitted that he obtained a cancer patient’s name, date of birth and Social Security number and used that information to get 4 credit cards in the patient’s name. Gibson also admitted that he used three cards to spend more than $9,000 on such items as video games, jewelry and home improvement supplies.
The HIPAA Privacy Rule allows for criminal penalties of up to 10 years in prison and $250,000 in fines when a person commits an offense with an intent to sell, transfer or use PHI for malicious harm. Gibson pled to a sentence bargain of 10 to 16 months.

2. University of Colorado v Denver Publishing

On August 2, 2004, a federal district court judge dismissed a lawsuit filed against a Denver newspaper for an alleged violation of HIPAA, 42 USC 1320d et seq. Judge Walker Miller found that the Rocky Mountain News’ publication of excerpts from a peer review report by the University of Colorado Hospital Authority did not create a private cause of action against the newspaper under HIPAA.

HIPAA protects patients’ privacy in medical records and allows the imposition of fines and possible jail time for anyone who violates the law with “intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm.”

V. RETENTION OF MEDICAL RECORDS

A. MICHIGAN MEDICAL RECORDS RETENTION ACT

On December 22, 2006, a new law was signed in Michigan which impacts the maintenance and retention of medical records. Key elements of the new law include:

1. Physicians who sell or close their practice, or otherwise cease to operate or practice must provide notice to the Michigan Department of Community Health specifying who will have custody of the records and how a patient may request access to or copies of his or her medical records. This requirement also applies when physicians sell their practices to another entity.

2. Physicians and other providers who are licensed under the Michigan Public Health Code are required to maintain a medical record for each patient.

3. Physicians must maintain medical records for a minimum of seven years, unless federal or state laws or regulations or generally accepted standards of medical practice require a longer retention period.

4. Physicians applying for a license or license renewal are required to include an affidavit with the application stating that he or she has a written policy for maintaining and protecting medical records and for otherwise complying with the legal requirements.
5. Failure to comply with these medical records maintenance and retention requirements could result in an administrative fine of $10,000.00.

Physicians should review and modify their medical record retention policies and procedures to ensure that they comply not only with this new law but with other applicable laws as well.

B. MEDICAL RECORDS: HEALTH FACILITIES GENERALLY

42 CFR § 482.24(b)(1): Inpatient and outpatient records must be retained in their original or legally reproduced form for at least 5 years.

MCL § 333.20175(1): A health facility or agency must keep and maintain a record for each patient, including a full and complete record of tests and examinations performed, observations made, treatments provided and, in the case of a hospital, the purpose of hospitalization.

MCL § 400.111b(8): Providers must retain records necessary to document fully the extent and cost of services, supplies or equipment provided to a medically indigent individual for 6 years after date of service.

C. AMERICAN MEDICAL ASSOCIATION, 1994 CODE OF MEDICAL ETHICS, 7.05(2)

1. AMA has actively supported and advocated the implementation of E-7.05.

2. Medical considerations are the primary basis for deciding how long to retain medical records. In deciding whether to keep certain parts of the record, an appropriate criteria is whether the physician would want the information if he/she were seeing the patient for the first time. For example, operative notes and chemotherapy should always be part of a patient's chart.

3. In all cases, if a particular record is no longer needed for medical purposes, medical records should be kept for at least as long as the length of time of the statute of limitations for medical malpractice.

4. If the patient is a minor, the statute of limitations may not apply until the patient reaches the age of majority.

5. Immunization records should always be kept.
6. Records of any patient covered by Medicare/Medicaid should be retained for at least 5 years.

7. Before discarding old records, patients should be given the opportunity to claim them or have them sent to another physician.

D. MEDICARE HOSPITAL MANUAL, CHAPTER 3 – ADMISSION PROCEDURES 301.3

Retain a copy of completed admission questionnaires to 10 years after the date of service which appears on the chart (in accordance with the DOJ's record retention requirements).

E. JCAHO 2000 ACCREDITATION MANUAL FOR HOSPITALS, IM.6.1

Retention time of record is determined by the hospital, based on law and regulation and the information's use for patient care, legal, research, and educational purposes.

F. MENTAL HEALTH SERVICES

42 CFR '412.27(c): Psychiatric unit must maintain medical records that permit determination of degree and intensity of treatment provided. No retention period is specified.

42 CFR '482.60(c): Psychiatric hospital clinical records must be maintained on all patients, including records sufficient to permit HCFA to determine degree and intensity of treatment furnished to Medicare beneficiaries.

42 CFR '482.24(b)(1): Hospital medical records must be retained in their original or legally reproduced form at least 5 years.

MCL '330.1141: A licensee under the Mental Health Code must maintain a complete record for each patient treated. No retention period is specified.

MCL '330.1746: A complete record must be kept current for each recipient of mental health services.

1998 Mich Admin Code R 330.1276: A licensed mental health hospital or unit must maintain current and accurate records and make them available for examination by the State. No retention period is specified.

1998 Mich Admin Code R 330.1276: A licensed mental health hospital or unit must maintain records and make them available for examination by the State. No retention period is specified.
G. HOME HEALTH AGENCY

42 CFR '491.10(c): Retain clinical records for 5 years after the month the cost report to which the records apply is filed with the intermediary, unless state law stipulates a longer period of time.

H. HOSPICE

42 CFR '418.74: Hospice must establish and maintain a clinical record for each individual receiving care and services. No retention period is specified.

1984 Mich Admin Code R 325.13109(1)(t)(v): Records must be retained for not less than 5 years after death or discharge.

I. LONG TERM CARE FACILITY

42 CFR '483.75(l)(2): Retain clinical records for the period required by state law or 5 years from date of discharge when there is no requirement in state law. For a minor, 3 years after the resident reaches legal age under state law.

1983 Mich Admin Code R325.21102(6): Retain clinical records for 6 years after discharge or 3 years after individual comes of age if a minor, whichever is longer.

1983 Mich Admin Code R 325.20113: A nursing home shall maintain for 3 years written complaints filed under its complaint procedure and all complaint investigation reports delivered to each complainant, and such records shall be available to the department upon request.

MCL '333.2172: The licensee shall retain for public inspection:

1. a complete copy of each inspection report of the nursing home received from the department during the past 5 years

2. a copy of each order or hearing pertaining to the nursing home issued by the department or a court for not less than 3 years after its date of issue or not less than 3 years after the date of resolution of the subject matter of the notice or order, whichever is later.

J. HIPAA

1. Notice of Privacy Practices

HCPs generally must provide individuals with adequate notice of the uses and disclosures of PHI that may be used by the HCP, and the
individual’s rights and the HCP’s legal duties with respect to PHI. These notices must be retained for at least 6 years from the date the notice was created or the date when it was last in effect, whichever is later. 45 CFR 164.520 and 45 CFR 164.530(i).

2. Policies and Procedures

HCPs must implement policies and procedures with respect to PHI that are designed to comply with the privacy regulations. These policies and procedures must be retained for at least 6 years from their date of creation or the date they are last in effect, whichever is later. 45 CFT 164.530(i)(1) and (j).

3. Consent Forms

Privacy regulations require certain entities to obtain an individual’s consent prior to suing or disclosing PHI to carry out treatment, payment or health care operations. These consent forms must be retained for at least 6 years from the date the consent form was created or the date the consent form was last in effect, whichever is later.

4. Authorizations

HCPs generally may not use or disclose PHI without an authorization. Authorizations must be retained for at least 6 years from the date the authorization was created or the date when it was last in effect, whichever is later.

VI. UNDERSTANDING AND NEGOCIATING EMR LICENSING AGREEMENTS

Electronic Medical Record Systems (EMR) can save a practice time and money, but the contracts that accompany them need to be reviewed just as carefully as the system itself. In reviewing the contract it there are 7 important areas to consider (1) software pricing, (2) term, (3) termination, (4) data ownership, (5) support services, (6) warranty, and (7) limitation of liability. The contracts can contain burdensome terms that can and should be negotiated prior to execution.

Pricing: Usually the contract is premised on one of the following three basic pricing approaches: (1) per computer (2) per user or (3) physical location. Each of the price approaches will work well for a particular type of practice. For example, a small practice with only a few computers but multiple users would be best suited for the per computer pricing. Conversely, if the practice will only have a few people with access to the EMR but in numerous workstations the per-user approach would be of more benefit. A larger practice would get the most benefit from a license that is for an entire physical location, which means that there would be no limit to the number of users or computers with accessibility. Vendors may tailor a contract to meet a practice’s specific needs, but it
has to be requested.

**Term, Termination and Data Ownership:** Always consider the term of the contract. The term can range from 10 years to a lifetime and often the contract does not allow for termination by the practice. If there is a termination date – what happens upon the end of the term? Is there a way to transfer the information from the system to another system? Will you be charged for the transfer? It is imperative that along with a term end date that the contract provides a way to retain the practices information. Also, the contract should make it clear that the data contained in the EMR is exclusively owned by the practice, so there is not an ownership dispute.

**Before you buy:** Ask the vendor if and how an EMR will protect physicians and produce legally sound records.

- Does the system assign authors to each new entry in a document? The system should not overwrite a prior author.
- Does the system record the time and identity of each user and what he or she looked at or changed?
- Are alterations to records obvious?
- How easily can an audit be performed? How accurate is the audit? The audit trails should not be alterable or easily disabled.
- Does the EMR allow “documentation by exception,” which allows the determined norms to be entered into the record unless otherwise changed?
- Does the EMR allow “open item billing,” which automatically bills when an order is made? If so, can it be disabled?
- Does the system have controlled access that provides different views dependent on the user's job title or department?
- Does the system allow cut-and-paste functions? If so, is the original source identified?
- If the system has click-box features, does it also allow free-text entry?

**Support:** EMR contracts typically contain support clauses, which may be available for a monthly fee or included in the overall contract price. The support that is offered can range from installation, training of staff, maintenance, telephone and on site support, supplying and installing software patches and updates. This section of the contract will also state what is required of the practice and may include storage requirements, update and patch installation requirements, service limitations, and installation requirements. The failure to comply with these may render the warranty for the software useless, so pay attention.

**Warranties and Limitation of Liability:** Warranties and liability clauses are the most difficult to negotiate. The warranties provided by the contracts can be incredibly limited. Many provide that the warranty is valid only when the system is unable to perform its basic functions. Make sure that the warranty is clear and defines exactly what it will and will not cover, so that you are informed and prepared. Lastly, the limitation of liability clauses can be severe and state that the vendor is not liable for failing to fulfill the
contract or for the software malfunctioning. This can limit your ability to recover damages in the future.

VII. ADVANCE DIRECTIVES AND ACCESS TO MEDICAL RECORDS

A. WHAT IS AN ADVANCE DIRECTIVE?

According to the Patient Self-Determination Act enacted by Congress, an “Advance Directive” is defined as follows:

. . . the term Advance directive means a written instruction, such as a living will or durable power of attorney for health care, recognized under State law (whether statutory or as recognized by the courts of the State) and relating to the provision of such care when the individual is incapacitated.

[42 USCS ' 1395cc(f)(3) (originally enacted as part of the Omnibus Budget Reconciliation Act of 1990, P.L. No. 101-508, ' 4206)].

Although a living will and a durable power of attorney differ in form, they essentially seek to achieve the same result — the advance self-determination of medical treatment by a patient in the event he or she becomes incapacitated. Essentially, a living will is a written document that is signed and witnessed stating the wishes of an individual concerning medical treatment decisions. The term Living will is a misnomer in the sense that it is not a will at all. Notably, living wills are not recognized by statute in Michigan. A durable power of attorney for health care on the other hand is a specific appointment of an individual (the agent) to make decisions regarding the health care of the patient (the principal) in the event of his or her incapacity. The durable power of attorney for health care has been adopted in Michigan.

B. THE DURABLE POWER OF ATTORNEY FOR HEALTH CARE IN MICHIGAN

Although Michigan does not have any specific legislation validating advance medical directives, Michigan did enact a law validating the durable power of attorney for health care effective December 19, 1990, which was completely restated by the Estates and Protected Individuals Code, which took effect on April 1, 2000. The durable power of attorney for health care provisions are now found at MCLA 700.5506-5512.

Essentially the Act provides that any person 18 years or older, who is of sound mind at the time of designation, may designate another person who is 18 years or older to exercise powers concerning care, custody and medical treatment decisions for the patient [MCLA ' 700.5506(1)]. This person is to
be known as a patient advocate [ld.]. The designation must be in writing signed and witnessed by two witnesses, who cannot be the spouse, parent, child, grandchild, sibling, presumptive heir, known devisee, physician, patient advocate, employee of a life or health insurance provider for the patient, employee of a health facility that is treating the patient, or employee of a home for the aged (as defined by Michigan law) where the patient resides. [MCLA '700.5506(3)]. Notably, the statute also requires that prior to implementation, the durable power of attorney for health care must be made a part of the patient=s medical record both with the attending physician and, if applicable, with the facility where the patient is located. [MCLA '700.5506(2)]. The designation may include a statement of the patient=s desires for care, custody and medical treatment and may authorize the patient advocate to exercise those powers which the patient could have exercised absent his or her disability. [MCLA '700.5507(1)].

The Act also provides that the patient advocate must sign the acceptance of the designation as a patient advocate (and successor advocate, if named) prior to implementation of the durable power of attorney for health care [MCLA '700.5507(3)]. The acceptance of the designation of patient advocate shall contain statement of the following:

1. This designation shall not become effective unless the patient is unable to participate in medical treatment decisions.

2. A patient advocate shall not exercise powers concerning the patient=s care, custody and medical treatment that the patient, if the patient were able to participate in the decision, could not have exercised on his or her own behalf.

3. This designation cannot be used to make a medical treatment decision to withhold or withdraw treatment from a patient who is pregnant that would result in the pregnant patient=s death.

4. A patient advocate may make a decision to withhold or withdraw treatment which would allow a patient to die only if the patient has expressed in a clear and convincing manner that the patient advocate is authorized to make such a decision and that the patient acknowledges that such a decision could or would allow the patient=s death.

5. A patient advocate shall not receive compensation for the performance of his or her authority, rights, and responsibilities, but a patient advocate may be reimbursed for actual and necessary expenses incurred in the performance of his or her authority, rights and responsibilities.
6. A patient advocate shall act in accordance with the standards of care applicable to fiduciaries when acting for the patient and shall act consistent with the patient’s best interests. The known desires of the patient expressed or evidenced while the patient is able to participate in medical treatment decisions are presumed to be in the patient’s best interests.

7. A patient may revoke his or her designation at any time and in any manner sufficient to communicate an intent to revoke.

8. A patient advocate may revoke his or her acceptance to the designation at any time and in any manner sufficient to communicate an intent to revoke.

9. A patient admitted to a health facility or agency has the rights enumerated in Section 20201 of the public health code, Act No. 368 of the Public Acts of 1978, being Section 333.20201 of the Michigan Compiled Laws.

[MCLA '700.5507(4)].

The authority under a designation shall not be exercised by patient advocate unless and until patient is unable to participate in medical treatment decisions [MCLA '700.5508(1)]. This is determined by the patient’s attending physician and another physician or license psychologist after examination of the patient. [Id.] These determinations shall be put in writing and shall be part of the patient’s medical record. [Id.]

If a dispute arises as to whether or not a patient is unable to participate in medical treatment decisions, a petition may be filed with the probate court in the county in which the patient resides. [MCLA '700.5508(2)] A court hearing will be made as soon as practicable and within 7 days after the receipt of the petition. [MCLA '700.5508(2)] If the court determines that a patient is unable to participate in medical treatment decisions, the authority, rights and responsibilities of the patient advocate shall become effective. [MCLA '700.5508(2)]

An individual designated as a patient advocate shall have the following authority, rights, responsibilities and limitations:

1. A patient advocate shall act in accordance with the standards of care applicable to fiduciaries in exercising his or her powers.

2. A patient advocate shall take reasonable steps to follow the desires, instructions, or guidelines given by the patient while the patient was
able to participate in care, custody, or medical treatment decisions, whether given orally or as written in the designation.

3. A patient advocate shall not exercise powers concerning the patient=s care, custody, and medical treatment that the patient, if the patient were able to participate in the decision, could not have exercised on his or her own behalf.

4. This designation cannot be used to make a medical treatment decision to withhold or withdraw treatment from a patient who is pregnant that would result in the pregnant patient=s death.

5. A patient advocate may make a decision to withhold or withdraw treatment which would allow a patient to die only if the patient has expressed in a clear and convincing manner that the patient advocate is authorized to make such a decision, and that the patient acknowledges that such a decision could or would allow the patient=s death.

6. A patient advocate under this section shall not delegate his or her powers to another individual without prior authorization by the patient.

[MCLA 700.5509(1)].

The durable power of attorney for health care is suspended if the patient regains ability to participate in medical treatment decisions [MCLA 700.5509(2)], and is revoked upon the death of the patient, an order of dissolution by the probate court, resignation or removal of the patient advocate(s) and revocation of designation by the patient, among others [MCLA 700.5510(1)].

Michigan law also has the following additional provisions:

1. Incapacity of patient

   Even if a patient is incapacitated and cannot participate in medical treatment decisions, his or her desires still prevail and he or she can change her mind regarding specific treatments or lack thereof and can even revoke the durable power of attorney for health care [MCLA 700.5511(1)].

2. Binding Effect

   A person providing care, custody and medical treatment to a patient is bound by sound medical practice and by the instructions of a patient
advocate, if the advocate complies with Michigan law [MCLA '700.5511(3)].

3. Petition to Probate Court

As noted above, a petition to probate court may be filed to make a determination of whether or not a patient is unable to participate in medical decisions and to determine whether or not a patient advocate is acting consistent with the patient=s best interests or in compliance with the statute [MCLA '700.5511(4)].

4. Pregnancy

A patient advocate cannot make a medical treatment decision under this statute which would result in the death of a pregnant patient. [MCLA '700.5512(1)].

5. Limitation on Health Care Provider

An HCP shall not require a designation to be executed as a condition of providing, withholding or withdrawing care, custody or medical treatment. [MCLA '700.5512(2)].

6. Limitations on Life and Health Insurance Companies

A life or health insurer cannot refuse to provide or continue coverage, limit coverage, charge a different rate or exclude coverage based on the execution or non-execution of a durable power of attorney for health care. [MCLA '700.5512(2)].

Notably, the statute specifically states that a durable power of attorney for health care shall not be construed to condone, allow, permit, authorize, or approve suicide or homicide. [MCLA 700.5512(4)]. This provision was specifically included so as not to confuse the durable power of attorney for health care with the activities of Jack Kevorkian, M.D.

VIII. ALTERATION AND DESTRUCTION OF MEDICAL RECORDS

A frequently asked question is whether medical records can be altered, and if so, in what manner. At first glance, the obvious answer would be “no.” However, upon further reflection, changes may need to be made in order for the record to be accurate. For example, there may have been an error when an HCP’s notes were transcribed, or an error may have been made when a patient’s medical information was inputted into a computer database. In each case, there is a right way and a wrong way to handle these types of issues.
A. OWNERSHIP OF MEDICAL RECORDS

At the outset, it is important to determine who owns the medical records of a patient. According to a somewhat dated opinion from the Attorney General, the physical record belongs to the HCP subject to the patient’s right of access to the medical records or the patient’s right to receive copies of the medical records. 1978 Opinion of the Michigan Attorney General No. 5125, May 30, 1978. This position, however, does not account for the fact that medical records are becoming increasingly computerized and stored on databases accessed by multiple HCPs. In such instances, who owns the records become less clear.

B. ALTERATION OF PATIENT RECORDS UNDER MICHIGAN LAW


By law, hospitals are charged with taking precautions to assure that the medical records are not wrongfully altered or destroyed. This provision does not bar any alterations, only those that are wrongful. As mentioned above, there may be instances where a modification to the record is required to ensure that it is accurate.

In some instances, an HCP and patient may agree that a medical record needs to be modified. However, there is authority stating that a hospital may not permit a doctor, even with the agreement of the patient, to change patient medical records unless the change is a supplementation or correction that does not cancel or alter a prior entry. 1994 Opinion of the Michigan Attorney General No. 6818, September 15, 1994.

2. What to do/ not do

a. If making changes, do not use white-out or erasers in medical records, and avoid blacking out any portion of the record

b. Do not replace pages or rewrite entire entries

c. Do use supplements to correct errors in the record

d. If you have to delete an entry, make a simple one-line strike through, and label, date and initial the correction

e. Do make changes in a timely fashion

f. Do note any new entries
3. **Computer Records**
   
a. By their nature, such records are subject to continuing alteration.

b. Such records should not be subject to continual alteration. Rather, the records should be authenticated and then no further changes made to them. As noted above, the records can be supplemented if errors or omissions are later discovered. However, this should be done in a timely fashion.

4. **Civil liability for Alteration of Medical Records**

   While there are no published cases on the matter, at least one panel of the Michigan Court of Appeals has recognized that there may be a private cause of action against a hospital or HCP for alteration of medical records. *Wilson v Sinai Grace Hospital*. In addition, some other jurisdictions have even gone so far as to permit the award of punitive damages. Perhaps more significant is the adverse inference that a court may allow to be drawn with respect to records that are wrongfully altered.

5. **Criminal/Administrative Liabilities**

   a. A hospital which is found to have wrongfully altered or destroyed medical records is subject to a civil fine of $10,000.00. MCL 333.20175(2).

b. An HCP or other person, knowing that the information is misleading or inaccurate, shall not intentionally, willfully, or recklessly place or direct another to place in a patient=s medical record or chart misleading or inaccurate information regarding the diagnosis, treatment, or cause of a patient=s condition.

   1. An HCP who intentionally or willfully violates this is guilty of a felony.

   2. An HCP who recklessly violates this is guilty of a misdemeanor, punishable by imprisonment for not more than 1 year, or a fine of not more than $1,000.00, or both.

c. Examples
i. There is at least one reported instance of a physician convicted of a misdemeanor attempted alteration of medical records.

ii. In 2000, a doctor’s license was suspended for 3 months after it was determined that he had a surgical consent altered and an office visit notation fabricated

C. UETA AND E-SIGN

The federal Electronic Signatures in Global and National Commerce Act (E-Sign) and Michigan's Uniform Electronic Transactions Act (UETA) (which was mandated by E-sign) encourage electronic transactions and paperless recordkeeping related to those transactions. Both acts provide that electronic records may be used to satisfy record retention requirements imposed under their laws so long as the electronic record accurately sets forth the information in the record and remains accessible to all persons entitled to access the record. These acts leave existing law in place but provide that records, signatures and contracts may be electronic, i.e., they shall not be denied validity because of the medium used in the transaction. Both acts require that the parties to the transaction consent to the use of electronic records. In addition, E-Sign contains stringent consumer consent requirements that must be met before electronic records can be used to provide a consumer with information that, under another law, must be available to the consumer in writing.

1. UETA

UETA provides that no contract may be denied enforcement or legal effect solely because it is memorialized with an electronic record or authenticated with an electronic signature. See MCL '450.831 et seq. Any law requiring that a record be retained is satisfied by retaining an electronic record if the electronic record:

a. accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

b. remains accessible for later reference. See MCL '450.842(1).

Even if a law requires that a record be retained in its original form, an electronic record retained in accordance with UETA satisfies that law. See id. However, UETA does not preclude a state governmental agency from specifying additional record retention requirements.

2. E-SIGN
E-Sign focuses on the validity of a transaction when important components of the transaction are in electronic form. E-Sign and UETA's record retention provisions are almost identical. E-Sign provides that if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information that:

a. accurately reflects the information set forth in the contract or other record; and

b. remains accessible to all persons entitled to access in a form capable of being accurately reproduced by later reference. See USC '7001(d).

Like UETA, even if a statute or other regulation requires that the contract or record be retained in its original form, that statute or regulation is satisfied by an electronic record that complies with this law. See id. As with UETA, certain exceptions apply to E-Sign that cannot be adequately covered in this memorandum. Please review the statute carefully to determine its applicability to your particular situation.

3. So what does it all mean?

a. Recognizes the use of electronic signatures in transactions

b. Would apply to health-related activities since it applies to the conduct of business or affairs between two people

c. Would not apply if there is no effect on interstate commerce

d. Does not require the use of electronic records or signatures

e. Does not mandate the type of electronic signature that must be used.

D. DESTRUCTION OF MEDICAL RECORDS

A common question often asked is how an HCP or facility should go about destroying medical records. As discussed previously, there are a myriad of retention requirements pertaining to various type of medical records. Additionally, issues such as malpractice also dictate when medical records should be destroyed.
While the timing of destruction of medical records will vary from patient to patient, each HCP and facility generating medical records should have some written policy in place to address the retention and destruction of medical records. A good policy will include the following:

1. Consideration of both paper and electronic records. With the proliferation of electronic records, a document retention and destruction policy that focuses solely on paper records will be inadequate.

2. Consideration to how records are to be retained. This includes considering whether certain records need to be filed, organized, archived or maintained in a different manner from other records.

3. Consideration to how records are to be duplicated. An HCP or entity may require certain records to be maintained in duplicate (this may be due to the need for accessibility or the importance of the records).

4. Compliance with applicable retention laws. This requires looking at both state and federal law to see what applies, and then appropriately documenting compliance with them.

5. Establishment of procedures for disseminating records. This is critical in several respects. First, it simply may not be necessary for all employees to have access to all records. Second, it may have legal implications (for example under HIPAA’s Privacy and Security Rules) if documents are accessed by those who have no legitimate reason to view such documents.

6. Development of programs to train employees about the record retention/destruction program so that it can be followed. Simply put, employees must know what to do with documents and management must regularly remind employees of how the policy works.

7. Designation of personnel to oversee the program.

8. Accountability for following the program. This entails providing a system for discipline in the event an employee fails to abide by the program.

9. Use of appropriate technological consultants. Any procedures for handling electronic documents, e-mail, rotation of back-up tapes and other issues raised by storage and use of electronic records should be “blessed” as reasonable.

10. Retention of all documentation relating to the development and implementation of the policy.
11. Development of the appropriate policy to notify patients of the destruction of records.

12. Development of a reliable mechanism that enables the company to suspend the destruction of documents upon notice of potential litigation, receipt of subpoenas, or an existing or potential government inquiry.

The program that is developed should be placed in writing, not only to provide written guidance to personnel but also to substantiate the existence of the program to appropriate regulatory bodies.

IX. PRIVILEGE/CONFIDENTIALITY

A. GENERAL RULE

In Michigan, physicians and HCPs may not disclose any information acquired in attending a patient in a professional capacity if such information was necessary to render treatment.

B. EXCEPTIONS/NUANCES

1. The identity of the patient is discoverable but the patient’s medical records are confidential.

2. The physician-patient privilege continues to exist after termination of the relationship.

3. The privilege of confidentiality survives the death of the patient.

4. Disclosure of medical records without the patient being identified may not violate the privilege.

5. A negligence claim against a physician generally brings the medical condition to issue.

6. An exception to the privilege may exist when there is a dangerous patient who makes physical threats of violence against third persons.

C. ADMINISTRATIVE PENALTIES

1. Disclosing information in violation of the privilege could constitute a violation of HIPAA.
2. Suspension or revocation of the HCP’s license if there is a "betrayal of a professional confidence." MCLA 333.16221.

D. COMMON LAW CAUSES OF ACTION

1. Invasion of privacy

Probably the most common allegation that arises in the context of improper disclosure of medical records is invasion of privacy. One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other. Restatement (Second) Torts 652A. Most of the cases have alleged that the invasion consisted of publicizing a matter concerning the private life of another if the matter publicized is of a kind that would be highly offensive to a reasonable person and is not of legitimate concern to the public. In Swickard v Wayne Medical Examiner, 438 Mich 536; 475 NW2d 304 (1991) the Michigan Supreme Court held that disclosure of an autopsy report and toxicology test results was not an unwarranted invasion of privacy and the physician-patient privilege (MCL 15.243(1)(c); MSA 4,1801(B)(1)(c)) did not apply.

2. Breach of fiduciary duty

Several courts in other jurisdictions have concluded that a physician has a fiduciary duty to the patient not to disclose the patient=s medical information and that the patient may recover damages for violation of the fiduciary duty. Courts have found the basis for this duty arising from common law principles, state statutes providing evidentiary privileges, state statutes providing for grounds to discipline physicians, the Hippocratic Oath and the AMA Principles of Medical Ethics. The duty is not absolute. Disclosure may be made without breach of the duty in circumstances in which the physician=s duty to the public supersedes his/her duty to the patient.

3. Breach of contract - express or implied

Although the courts have primarily addressed unauthorized disclosures of medical information as tort cases, patients have occasionally alleged that a provider who discloses a patient=s medical information has breached a contract with the patient to hold the patient=s medical information confidential. The cases that have been reported thus far have alleged an implied contract; however, in the health plan contract an express contract might be alleged.

Many contracts between health plans and providers obligate both parties to hold medical information confidential in accordance with
state and federal law. Disclosure of a patient’s medical information that is contrary to state or federal law would violate that contractual provision (see e.g. Notice of Privacy Policy). Whether the patient could enforce the breach depends on whether the patient is a third party beneficiary of that contractual provision. While most health plan provider contracts provide that no party is intended to be a third party beneficiary, it is at least possible that a court could reach a contrary conclusion based on state law principles of third party beneficiary contracts.

In addition, documents issued by health plans to beneficiaries, such as evidences of coverage, sometimes contain provisions stating that the member’s medical records and related information will be kept confidential. Care should be taken in drafting these provisions so that they do not promise a greater degree of confidentiality than is required by state law.

4. Negligence

Improper disclosure of a patient’s medical records may constitute negligence. The elements for a cause of action for negligence are:

a. the existence of a duty, i.e. an interest that is protected against unintentional invasion,

b. breach of duty, i.e., conduct that falls below the standard established by law for the protection of others against unreasonable risk of harm,

c. causation of harm, i.e., the breach of duty must be a legal cause of damages, and

d. proximate (legal) cause.

See Restatement (Second) Torts 281, 282.

In the context of disclosure of a patient’s medical records, the duty may be imposed by several sources. Applicable statutes and regulations discussed above may form the basis for a duty of nondisclosure by particular persons. The existence of a fiduciary relationship between parties, such as between a patient and physician, may also form the basis for a legal duty. Similarly, the ethical guidelines promulgated by associates, which support the notion of the existence of a fiduciary relationship, may form the basis for a duty.
Whether a particular action constitutes a disclosure in breach of duty would be determined based on the facts of the disclosure merely segregating certain files under circumstances which would suggest the existence of a medical problem might be viewed as disclosure. Compliance with applicable laws and regulations would be relevant as to whether a particular disclosure comprised a breach of duty. Causation, harm and proximate cause would be determined under traditional principles of tort law.

5. Defamation

A few cases relating to disclosure of medical information have alleged defamation. The elements of a defamation action are:

a. a false and defamatory statement concerning another;

b. an unprivileged publication to a third party;

c. fault amounting to at least negligence on the part of the publisher; and

d. either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication.

Restatement (Second) Torts ’ 558.

Perhaps the issue most likely to arise in the context of a defamation case arising out of disclosure of medical information is whether the information disclosed is, in fact, false. Publication of inaccurate information about a person’s medical condition has been historically a common basis for defamation actions, although it is outside the scope of this presentation, which is about confidentiality of a patient’s actual information.

The second issue that is likely to arise is whether the publication is privileged. For the existence of privilege, in addition to common law privileges, confidentiality statutes have likely created privileges for certain disclosures.

6. Negligent Infliction of Emotional Distress

Negligent infliction of emotional distress is essentially a subcategory of negligence, which is recognized in some jurisdictions. The issue is the nature of the harm that may be compensable. Under the Restatement (Second) of Torts, a person who unintentionally causes
emotional distress to another is liable for the resulting illness or bodily harm if the person:

a. should have realized that his conduct involved an unreasonable risk of causing the distress to that person;

b. from the facts known to that person, should have realized that the distress if it were caused, might result in illness or bodily harm.

Restatement (Second) of Torts ‘313. Generally, there is no liability for distress only, in the absence of bodily harm. Id. comment a.

7. Intentional Infliction of Emotional Distress

In certain cases, a person whose medical information has been improperly disclosed might be able to allege intentional infliction of emotional distress. Generally, proving this tort requires a plaintiff to show that the defendant has intentionally or recklessly engaged in extreme and outrageous conduct that caused severe emotional distress. Restatement (Second) of Torts ‘46.

8. Breach of Duty to Disclose

In a growing number of jurisdictions, the courts have imposed on providers a duty to warn third parties if the medical condition of the patient creates a hazard for the third party. The seminal case is Tarasoff v Regents for the University of California, 551 P.2d 334 (1976), which held that a psychotherapist had an affirmative duty to warn the patient’s intended victim when the provider reasonably believed that the patient would cause serious bodily harm or death, and that failure to warn constituted negligence.

The rationale of the Tarasoff case has also been applied in the context of potential HIV infection. A California case held that a medical group could be sued for failing to warn patients that one of the practice’s gynecologists was HIV positive, even though California law imposes civil and criminal penalties (including one year jail time) for each unauthorized disclosure. Amaral v Gordon, No. 126484 (Los Angeles County, Cal Super. Ct. 1990) cited in DeWitt ‘16.04[3][e][iii]. Similarly in West Virginia, a hospital was found liable for failure to warn a hospital security guard about a new patient who bit the guard. The guards were usually warned about HIV status in order to take proper precautions. The guard was awarded $2 million, even though the guard had not tested positive, based on an emotional distress claim. Johnson v West Virginia, 13 SE2d 889 (WVa 1991).

In a few cases, plaintiffs have alleged that they have direct cause of action under one or more regulatory statutes. To date, courts seem to be rejecting these claims. It is unclear whether a person whose substance abuse records are disclosed may be able to sue private persons for damages.

10. ERISA - Preemption and Liability

State law causes of action for improper disclosure against health plans in the course of administering a health benefits plan governed under the Employee Retirement and Income Security Act of 1974 as amended (ERISA) might be preempted. Most federal courts considering claims against health plans arising out of the administration of their health benefits programs have concluded that ERISA preempts state law tort and contract claims against health plans.

A claim could be made that unauthorized disclosure comprised a breach of a health plan’s (or employer’s) fiduciary obligations under ERISA. Fiduciaries are required to discharge their duties with respect to a plan solely in the interest of the participants and beneficiaries and with the care, skill, prudence, and diligence [of] . . . a prudent man acting in a likely capacity and familiar with such matters. @ 29 USC 1104(a)(2).

However, even assuming that a health plan was considered to be an ERISA fiduciary, it is not clear whether an aggrieved member would have any effective form of relief. Courts have historically declined to award extracontractual or punitive relief in ERISA cases.

X. HIPAA – STATE LAW PREEMPTION AND SUMMARY OF HIPAA AND STATE LAW DIFFERENCES

A. GENERAL RULE

General rule: “A standard, requirement or implementation specification . . . that is contrary to a provision of State law preempts the provision of State law.” Privacy Rule, Section 160.203. A state law provision is contrary to a HIPAA provision if a covered entity would find it impossible to comply with both the state and federal requirements; or if the state law stands as an obstacle to the accomplishment and execution of the full purposes of HIPAA.

B. EXCEPTIONS
The Secretary of DHHS may make a determination that the provision of state law applies if it:

- Is necessary to prevent fraud and abuse related to the provision of or payment for health care;
- Is necessary to ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
- Is necessary for state reporting on health care delivery or costs;
- Is necessary for purposes of serving a compelling need related public health, safety, or welfare, and, if a standard or specification under part 164 of HIPAA is at issue, if the Secretary of DHHS determines that the intrusion into privacy is warranted when balanced against the need to be served;
- Has as its principal purpose the regulation of the manufacture, registration, distribution or other control of any controlled substances;
- Relates to the privacy of health information and is more stringent than a standard or specification of HIPAA;
- Provides for the reporting of disease or injury, child abuse, birth, or death, or for the conduct of public health surveillance, investigation or intervention; or
- Requires a health plan to report or provide access to information for management or financial audits, program monitoring and evaluation, or licensure or certification.

A state law provision is more stringent than a HIPAA provision if the state law provision would prohibit a use or disclosure that would be otherwise permitted by HIPAA or if the state law provides greater privacy protection for the patient.

C. SPECIFIC EXAMPLES

1. MCR 2.314- This Michigan Court Rule permits the release of medical information pursuant to subpoena or court order.

Both HIPAA and the Court Rule apply with respect to a court order, as both permit the release of PHI pursuant to a court order. If a subpoena but there has been no waiver of the privilege, Michigan law applies because it precludes disclosure absent an express waiver of
privilege. On the other hand, if there has been a waiver, HIPAA would apply because its requirements regarding subpoenas are more stringent.

2. **MCLA 257.625a** - Disclosure of chemical breath results to prosecutor is permitted.

Both HIPAA and Michigan law apply because both permit disclosure when required by law and for law enforcement purposes.

3. **MCLA 259.187** - Blood test for alcohol or other drugs to be made available to affected individual and prosecutor.

Both HIPAA and Michigan law apply because both permit disclosure to the affected individual and when required by law and for law enforcement purposes.

4. **MCLA 330.1143a** - Records and data compiled for review functions of a psychiatric hospital are not subject to a court subpoena.

HIPAA does not specifically address the disclosure of peer review records, so such records could be obtained via a subpoena or court order. However, Michigan law applies as it is more stringent than HIPAA.

5. **MCLA 330.1498i** - A parent or guardian shall be notified upon the hospital admission of minor.

Both HIPAA and Michigan law apply because both permit disclosure to parents or guardians where permitted by Michigan law.

6. **MCLA 330.1707** - Parent or guardian need not be notified of mental health services provided to minor unless determination of compelling need and notification of minor of intent to disclose.

Both HIPAA and Michigan law apply because both permit disclosure to parents or guardians where permitted by State law.

7. **MCLA 330.1748(5)** - Confidential mental health records may be disclosed pursuant to a court order or subpoena to the extent the information is not privileged.

Both HIPAA and State law apply with regard to court orders, as both permit disclosures pursuant to court orders. HIPAA applies as to subpoenas because HIPAA requires additional safeguards beyond what Michigan law provides.
8. **MCLA 330.1748(5)**: Confidential information relating to mental health records may be disclosed to a surviving spouse or other relative for purposes of applying for or receiving benefits.

HIPAA applies, as it allows disclosure only to persons who have authority to act on behalf of the deceased’s estate.

9. **MCLA 330.1748(7)**: Mental health information may be disclosed by the holder of the records for purposes of research, evaluation, accreditation or statistical compilation, and the identity of the person may be disclosed under certain circumstances.

HIPAA applies, as it would an authorization or authorization waiver from an Institutional Review Board or privacy board.

10. **MCLA 330.1748(7)**: PHI may be disclosed to a mental health provider or public agency if a compelling need for disclosure exists, based on probability of harm to patient or others.

Both HIPAA and Michigan law apply as both allow disclosure to avert a threat to an individual or the public.

11. **MCLA 333.18513**: An authorization is required for disclosures by certified social workers unless pursuant to a duty to warn.

Michigan law applies, as HIPAA permits disclosure for TPO without an authorization.

12. **MCLA 333.22210**: A short-term facility must make records available within a reasonable period of time not to exceed seven (7) days.

Michigan law applies, as it requires the availability within seven days whereas HIPAA provides thirty (30) days.

13. **MCLA 331.531**: PHI may be disclosed to peer review entities.

Both HIPAA and Michigan law apply as to PHI that does not include psychotherapy notes, as HIPAA allows disclosure as part of TPO and State law allows disclosure.


Both HIPAA and Michigan law apply as both permit disclosure for public health purposes.

15. **MCLA 333.5127**: Informing spouse or parent of minor regarding treatment given to or needed by minor for HIV.
Both HIPAA and Michigan law apply as to disclosures to parents or guardians, as HIPAA defers to Michigan law for disclosure of PHI to parents or guardians; HIPAA applies as to disclosures to spouse, as HIPAA would allow the patient to object to such disclosure.

16. **MCLA 333.9132** - Health facility providing prenatal and pregnancy-related care to minor shall inform the minor that the parent or guardian of the minor may be informed of the care.

Both HIPAA and Michigan law apply as HIPAA defers to State law in provision of PHI to parents or guardians.

17. **MCLA 600.2157** - Waiver of physician/patient privilege as to medical malpractice actions.

HIPAA applies as it only permits disclosure of PHI in response to a court order or if the patient has been given an opportunity to object and assert the privilege.

18. **MCLA 722.30** - Noncustodial parent shall not be denied access to child’s medical records.

Both HIPAA and Michigan law apply as HIPAA defers to State law in provision of PHI to parents or guardians.


Both HIPAA and Michigan law apply as HIPAA defers to State law with respect to reporting obligations, and HIPAA allows disclosure in cases of abuse.

20. **Attorney General Opinion No. 6439** - Director of FIA may request PHI from a provider relating to a claim.

Both HIPAA and Michigan law apply as both allow disclosure of PHI to ensure compliance with government-funded benefit programs.

21. **Attorney General Opinion No. 6369** - Hospital or health care organization has no duty to inform next-of-kin regarding organ donations.

Michigan law applies, as no HIPAA counterpart exists; however, HIPAA generally allows the disclosure of PHI for purposes of autopsy or organ donation.
22. **Attorney General Opinion No. 5709** - County community mental health board may obtain treatment records of persons receiving mental health treatment.

Both HIPAA and Michigan law apply as both allow disclosure for public health purposes and oversight.

23. **Attorney General Opinion No. 5125** - Provider may establish and implement a policy for regulating a patient’s access to his or her records.

Both HIPAA and Michigan law apply as both require covered entities to establish procedures for patient access and each permits reasonable limitations on such access.

24. **Rule 325.3828** - Informed consent necessary prior to surgery being performed by any freestanding surgical outpatient facility.

Michigan law applies as there is no HIPAA rule regarding consent for surgical procedures.

25. **Rule 325.6405** - HMO contract must provide confidentiality covenants

Both HIPAA and Michigan law apply as both require PHI to be maintained in a confidential manner.

26. **Rule 325.20112** - Nursing home must develop and publicly post its policies relating to patient rights to access of records.

Both HIPAA and Michigan law apply as both require a covered entity to develop and maintain policies regarding patient access to records.

XI. **MICHIGAN AIDS LEGISLATION**

A. **CONSENT AND HIV TEST COUNSELING**

Physicians who order HIV tests or health facilities performing HIV tests, must provide appropriate counseling before and after the test is administered. Generally, HIV tests may not be ordered for the purpose of diagnosing HIV infection without first receiving written informed consent of the test subject. Written informed consent consists of a signed writing executed by the test subject and includes an explanation of the test, the test subject’s rights, and a list of persons to whom test results may be disclosed. Additionally, test results must be disclosed to test subjects on the forms provided by the Department. Consent for HIV testing is not required if the patient is informed in writing upon admission to a health care facility that the test may be
performed without written consent and the test is performed after a health professional sustains mucous membrane or open wound exposure to blood or other body fluids of the patient. MCLA '333.5133.

B. REPORTING REQUIREMENTS

A person or governmental entity obtaining a test result indicating a subject is HIV infected, must report the following to the Michigan Department of Public Health:

1. the name and address of the person or governmental agency submitting the report;
2. the age, race, sex and country of residence of the test subject;
3. the date on which the test was performed;
4. the test result;
5. if known, whether the subject has tested positive for HIV on a previous occasion;
6. probable method of transmission; and
7. the purpose of the test.

The required information must be sent to the Department within 7 days after obtaining the test result on a form provided by the Department. The same information must also be submitted to the appropriate local health department. However, unlike the report sent to the Michigan Department of Public Health, the name, address and telephone number of the test subject must be included in the report to the local health department. Individuals tested in a physician=s private practice office, or office of a physician employed by or under contract to a health maintenance organization may request that their name, address and telephone number not be disclosed. Subject to the rules on partner notification, physicians must comply with this request. MCLA '333.5114.

C. PARTNER NOTIFICATION

HIV infected individuals must notify sexual or hypodermic needle-sharing partners of positive test results. The infected individual may request his physician to notify the partner. A person administering a test for HIV or an antibody to HIV to an individual must refer the individual to the local health department for assistance with partner notification if the test result indicates that the individual is HIV infected and the person determines that he
individual needs assistance with partner notification. This information may, if necessary, include the name, address and telephone number of the individual test subject. MCLA '333.5114a.

D. CONFIDENTIALITY REQUIREMENTS

All reports, records and data pertaining to HIV testing, treatment and partner notification are confidential and subject to the physician / patient privilege. A court may order disclosure of confidential HIV information only when certain statutorily enumerated criteria are satisfied. Confidentiality does not apply to the following:

1. Information disclosed to a health department to protect the health of an individual, to prevent further transmission of HIV, or to further diagnose and care for a patient.

2. Information concerning an individual with HIV if disclosed by a physician to another individual known to be a contact of the HIV infected individual if the physician determines that disclosure is necessary to prevent a reasonably foreseeable risk of further HIV transmission. Physicians have an affirmative duty to make such disclosure and may discharge this affirmative duty by referring the HIV infected individual to the local health department for partner notification assistance.

3. Disclosure is expressly authorized in writing, which is specific to HIV. Written authorization may be executed by a parent or legal guardian of a minor or incapacitated person.

4. Information required to be included in a report under the Michigan Child Protection act.

5. Where such disclosure is otherwise provided by law.

Generally, disclosure, unless by written authorization, may not identify the HIV infected individual unless the person making the disclosure determines that it is reasonably necessary to present a foreseeable risk of HIV transmission. Persons disclosing HIV test results as provided above are immune from civil or criminal liability and administrative penalties.

A violation of the confidentiality requirements noted above is a misdemeanor punishable by imprisonment for up to one year or a fine of not more than $5,000 or both. Actual damages, including reasonable attorney’s fees, may also be awarded in civil actions. MCLA '333.5131.

E. MARRIAGE APPLICANTS
Individuals applying for a marriage license are required to obtain written educational materials prepared by the Department from the county clerk regarding prenatal care and the transmission and prevention of venereal disease and HIV infection. The written educational materials must describe the availability to the applicant of tests for both venereal disease and HIV infection, and include a list of locations where HIV counseling and testing services funded by the Department are available.

An applicant must sign and file with the county clerk an application for a marriage license that includes a statement with a check-off box indicating that the applicant has received the educational materials regarding the transmission and prevention of both venereal disease and HIV infection and has been advised of testing for both venereal disease and HIV infection. If an applicant does undergo HIV testing and the results come back positive, the person administering the test must inform both applicants of the test results and provide counseling for both applicants regarding the modes of HIV transmission, the potential for HIV transmission to a fetus, and protective measures.

F. PREGNANCY

At a pregnant woman=s initial examination, a physician must submit test specimens to an approved laboratory to perform tests for HIV unless in the physician=s professional opinion the tests are medically inadvisable or the patient does not consent. Physicians must make and retain a record showing the date the tests were ordered, and the test results. If the tests were not ordered, the record must contain an explanation. Although these records are not public, they must be available to the local health department and to a physician providing medical treatment to the woman. MCLA '333.5123.

G. MINOR=s CONSENT TO TREATMENT FOR HIV

The consent to treatment of a minor who has or is believed to have venereal disease or HIV is valid as if the minor has obtained the age of majority. The treating physician may, but is not obligated to, inform the minor=s parents or guardian that treatment has been given or is needed. The information may be given or withheld without the minor=s consent. MCLA '333.5127.

H. BLOOD AND ORGAN DONATIONS

An HCP who procures human blood, tissue, organs, or other specimens for transplantation or transfusion must test each donor or sample for HIV. Testing is not required if, due to exigent circumstances, it cannot be performed during the time in which the specimen is viable for transplantation.
or transfusion. If the HIV test results are positive, the specimen may not be used for transplantation or transfusion. If there is insufficient time to perform the test due to exigent circumstances, the recipient and physician must be so informed and both must agree in writing to use the specimen. If the recipient is unable to give informed consent, the recipient=s spouse, adult son or daughter, parent, adult brother or sister, or guardian may consent. Donors must also be informed of positive test results. MCLA ' 333.9123.

I. ARTIFICIAL INSEMINATION

Health facilities or agencies licensed to provide artificial insemination on an anonymous basis shall use only frozen sperm and must test each potential donor for the presence of HIV or an HIV antibody before frozen sperm may be used for artificial insemination, and not less than 6 months after the date of donation, a second blood sample must be taken and tested. If any test results are positive, the sperm may not be used.

J. EMERGENCY CARE

If an emergency patient is assisted or transferred to a health facility by a police officer, fire fighter, emergency medical technician, or licensed paramedic, and if the patient tests positive for an infectious agent, the facility must notify the police officer, fire fighter, emergency medical technician, or licensed paramedic, and if the patient tests positive for an infectious agent, the facility must notify the police officer, fire fighter, emergency medical technician, or licensed paramedic. The health facility must not reveal that the infectious agent is HIV unless requested by the individual in writing. Such notice shall not identify the emergency patient. Individuals who are authorized or required to give such notification are immune from civil or criminal liability when acting in good faith. MCLA ' 333.20191.

XII. SUBPOENAS

A. INTRODUCTION

HIPAA neither expressly prohibits nor permits the disclosure of PHI in response to subpoenas. Court orders, subpoenas, and other legal requests for PHI are not a “mandatory disclosure” under HIPAA. Mandatory disclosures are limited to requests from the individual that is the subject of PHI, and from the U.S. Department of Health and Human Services. Subpoenas and court orders fall within the more limited realm of “permissive” disclosures, which may be made so long as certain protections are met prior to disclosure.

In litigation, there are generally four ways to obtain medical records under HIPAA. The first is to obtain an authorization from the person whose PHI is
sought, and provide it along with a subpoena. As a separate authorization is needed for each covered entity, an authorization will need the specific name of the covered entity from which the PHI is being sought. An authorization containing generic names such as “any and all medical care providers for plaintiff” will not be sufficient and is inappropriate. As will be discussed later on in these materials, a demand for ex parte interviews may be included as part of the authorization, together with notice to the medical care professional that he/she need not engage in such an interview.

If a party does not have an authorization, it can: (1) Obtain a court order as set forth in 45 CFR §164.512(e)(1)(i); (2) Send a subpoena or discovery request where a plaintiff has been given notice pursuant to 45 CFR §164.512(e)(1)(ii)(A); or (3) Send a subpoena or discovery request where reasonable effort has been made to obtain a qualified protective order pursuant to 45 CFR §164.512(e)(1)(ii)(B).

A party receiving a subpoena has two options for compliance with a subpoena. The first, a “qualified protective order,” is most easily accomplished when the HCP or other covered entity is a party to the litigation. This method requires that the parties to the dispute agree to a qualified protective order and present it to the court or administrative tribunal. Generally, a court will enter an order whenever both parties agree to it, and therefore the parties do not have to wait for the order to be entered before producing the PHI. A qualified protective order permits the parties to freely exchange PHI that is relevant to the litigation without obtaining individual authorizations or giving individual notice, so long as the parties agree to restrict use of the PHI to the matter of the litigation, and to not further disclose PHI.

Obtaining agreement by all parties to a protective order is difficult when the covered entity is not a party to the litigation, and in such cases the second option, the “notice requirement,” may be preferable. This opinion requires that the requesting party give the HCP a written statement and supporting documentation to establish that the requesting party has (1) made a good faith effort to provide written notice to the individual whose PHI is requested, (2) the notice included sufficient information about the litigation or proceeding to permit the individual to raise an objection before the appropriate court, and (3) the time for the individual to raise objections has elapsed and either no objections were filed or all objections were resolved by the court, meaning that the court found that the PHI may or should be disclosed.

What is a “good faith attempt” to provide written notice to an individual? At a minimum, this is simply mailing a copy of the subpoena to the individual's last known address. If the written notice is mailed to the individual at the same time as the service of the subpoena upon the HCP, then a period of time will have to elapse before the requesting party can fulfill the requirement of a “written statement that the time for the individual to raise objections to the
court has elapsed and no objections were filed.” Although the covered entity should be able to rely upon the requesting parties “written statement,” the entity could also check with the court to confirm whether sufficient time has passed and either no objections were filed, or all objections were rejected by the court.

That being said, as previously noted, HIPAA gives way to state law where state law is more restrictive. In this case, Michigan law generally prohibits the disclosure of a patient’s medical records except in those cases where the patient is a party. To start, Michigan recognizes the Physician-Patient Privilege Statute (MCLA 600.2157). Additionally, the Patient Rights Statute (MCLA 333.20201) provides in part that “a third party shall not be given a copy of the patient’s or resident’s medical record without prior authorization of the patient or resident.” Accordingly, if neither the patient nor the covered is a party to a suit, and absent a HIPAA-compliant authorization, a covered entity may not want to take on the burden of confirming that the parties have truly complied with all the steps for production in response to a subpoena, particularly where it appears the individual objects to the disclosure. In such cases, the covered entity should notify the court and the parties that it is not attempting to interfere with the court proceedings, but that it prefers to have a direct court order for production of the records in order to fully comply with the HIPAA privacy regulations.

As mentioned previously, HIPAA compliance is not sufficient if state laws are violated. Courts have already addressed the application of the HIPAA privacy rules for disclosures in judicial proceedings. The most well publicized case, National Abortion Federation v Ashcroft, dealt with the Department of Justice’s request for disclosure of patient abortion records. The Department of Justice’s order permitted the hospitals to remove certain information from the records, including patient names and addresses, but not the patient’s medical history or state of residence. The Court ruled that HIPAA did not prohibit the disclosure to the Justice Department because HIPAA’s privacy rules permit the disclosure of PHI pursuant to a court order. However, the court found that Illinois’ medical privacy law provided more stringent protection for patient records and prohibited the disclosure of the records. The government attempted to argue that the state law was trumped by federal common law and that HIPAA’s permissive disclosure of the records overruled the Illinois prohibition on disclosure of the records. However, the court noted that HIPAA provided for the application of more stringent state laws, and therefore the Illinois law was not preempted by HIPAA and the records could not be disclosed.

Michigan’s medical privacy rules strictly regulate the disclosure of certain health information including communicable diseases including HIV/AIDS, mental health and substance abuse treatment. A court order is only a permissive disclosure under HIPAA, and if the covered entity is concerned that disclosure may violate HIPAA or other privacy regulations, the covered
entity could insist upon receiving an individual authorization for the disclosure. If the individual is a party to the litigation, a court may always order the individual to sign an authorization for the disclosure. The HCP not only may, but must, disclose records requested with an individual authorization.

B. **REQUIREMENTS OF A SUBPOENA**

\$ must be entitled in the name of the People of the State of Michigan; and

\$ must be imprinted with the seal of the Supreme Court of Michigan, or

\$ must be issued by a federal court.

1. **Subpoena Requesting Production of Medical Records**

   a. must be accompanied by properly executed authorization signed by patient

      i. deceased patients - authorization by personal representative of estate

      ii. minors - by parent or legal guardian

   b. subpoena not required for production of records if there is:

      i. a court order

      ii. the request for records is accompanied by a HIPAA-compliant authorization

   c. respond to request within 28 days, unless otherwise specified in subpoena or order of court (MCR 2.314, MCR 2.310)

      i. notify the patient if no authorization is provided;  

      ii. make information reasonably available for inspection or copying; or

      iii. deliver a true and exact copy of requested information

\& sworn certificate of completeness

\& entitled to reasonable reimbursement in advance
iv. must permit reasonable inspection of original document if requested

v. records incapable of reproduction (i.e. x-rays):

   - inform party making request - may require signed receipt indicating records will be returned after reasonable time for inspection

2. Subpoena Requesting Appearance or Production of Records at Trial (MCR 2.506)

   a. Subpoena must also include:

      i. the name of the court in which the matter is pending;

      ii. the place where the trial or hearing is scheduled;

      iii. the title of the action in which the person is expected to testify;

      iv. the file designation assigned by the court;

      v. a statement that failure to obey the subpoena or reasonable directions as to time and place to appear may subject the recipient to penalties for contempt of court; and

      vi. also make sure proper authorizations have been provided.

3. Service of Subpoena (MCR 2.105, MCR 2.506(G))

   a. A subpoena may be served personally, by registered or certified mail, or by mailing a copy of the subpoena and a postage prepaid card acknowledging service to the witness.

   b. The fee for one day=s attendance and mileage provided by law must be tendered at the time of service, or, if indicated on an acknowledgment card, after separate appearance at court.

   c. Service on attorney or party (MCR 2.107). Fees and mileage not paid in advance

4. Compliance with Subpoena

61
a. A person must comply with a subpoena unless relieved by order of the court or written direction of the person issuing the subpoena. (MCR 2.506(H)). A failure to comply with a subpoena may be considered a contempt of court by the court in which the action is pending. (MCR 2.506(E)).

b. If a party fails to comply with a subpoena, the court may stay further proceedings, tax costs to the party, strike all or a part of the pleadings of that party, refuse to allow that party to support or oppose designated claims and defenses, dismiss the action, or enter a judgment by default against that party.

c. Attendance by custodian of records required if requested.

d. If only records are requested, copies may be sent unless an original is specified. Hospitals may deliver copies of records to clerk of court with sworn certificate. Attorney who issued subpoena must be promptly notified. (MCR 2.506(I)).

XIII. ELECTRONIC TRANSMISSION AND SECURITY STANDARDS

A. OVERVIEW

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](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 (“EPHI”).

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.

B. THREE STEPS TO COMPLIANCE

The new rule on the security of electronic patient records boils down to 3 sets of standards 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

C. 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.

D. GENERAL SECURITY STANDARDS

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

1. Ensure the confidentiality, integrity, and availability of all EPHI the covered entity creates, receives, maintains, or transmits;

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

3. Protect against any reasonably anticipated uses or disclosures of such information that are not otherwise permitted or required by the Privacy Rule; and

4. 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 its rationale for its decision. Where a security standard has no implementation specifications, the standard itself serves as an implementation specification.

E. 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, rewore 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.

1. 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.

2. Workforce Security

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

3. 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.

4. 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.

5. 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.

F. 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.

1. 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.

2. 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.

3. 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.

G. 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.

1. 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.

2. 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.

3. Integrity

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

4. 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.

5. 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.

H. 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:

1. 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;

2. ensure that any agent to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it;

3. report to the covered entity any security incident of which it becomes aware;

4. 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
5. 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:

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

I. 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.

J. QUESTIONS AND ANSWERS

1. **Question:** Does the HIPAA Security Rule apply to written and oral communications?

   **Answer:** No. The Security Rule is specific to EPHI. It should be noted however that EPHI also includes telephone voice response and faxback systems because they are used as input and output devices for computers. EPHI does not include paper-to-paper faxes or video
teleconferencing or messages left on voice mail, because the information being exchanged did not exist in electronic form before the transmission. In contract, HIPAA Privacy Rule addresses all mediums of PHI, including written and oral. Information on the Privacy Rule can be found online at: http://www.hhs.gov/ocr/hipaa/.

2. **Question:** Does the HIPAA Security Rule require the use of an electronic or digital signature?

**Answer:** No. The Security Rule does not require the use of electronic or digital signatures. However, electronic or digital signatures could be used as a security measure if the covered entity determines their use is reasonable and appropriate. Additionally, the final rule to adopt a HIPAA standard for electronic signatures has not yet been published. Consequently, the implementation of an electronic signature standard currently is not required.

3. **Question:** Do the HIPAA Security Rule requirements for access control, such as automatic logoff, apply to employees who telecommute or have home-based offices if the employee accesses EPHI?

**Answer:** Yes. Covered entities that allow employees to telecommute or work out of home-based offices and have access to EPHI, must implement appropriate safeguards to protect the organization’s data. The automatic logoff implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the logoff implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate, or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure. The information access management and access control standards, however, require the covered entity to implement policies and procedures for authorizing access to EPHI and technical policies and procedures to allow access only to those persons or software programs that have been appropriately granted access rights.

4. **Question:** How will we know if our organization and our systems are compliant with the HIPAA Security Rule’s requirements?

**Answer:** The purpose of the final Security Rule is to adopt national standards for safeguards to protect the confidentiality, integrity, and
availability of EPHI that is collected, maintained, used or transmitted by a covered entity. Compliance is different for each organization and no single strategy will serve all covered entities.

Covered entities should look to § 164.306 of the Security Rule for guidance to support decisions on how to comply with the standards and implementation specifications contained in §§ 164.308, 164.310, 164.312, 164.314, and 164.316. In general, this includes performing a risk analysis; implementing reasonable and appropriate security measures; and documenting and maintaining policies, procedures and other required documentation.

Compliance is not a one-time goal, it must be maintained. Compliance with the evaluation standard at § 164.308(a)(8) will allow covered entities to maintain compliance. By performing a periodic technical and non-technical evaluation, a covered entity will be able to address initial standards implementation and future environmental or operational changes affecting the security of EPHI.

5. **Question**: What does the HIPAA Security Rule mean by physical safeguards?

**Answer**: Physical safeguards are physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment from natural and environmental hazards, and unauthorized intrusion. The standards under physical safeguards include facility access controls, workstation use, workstation security, and device and media controls. The Security Rule requires covered entities to implement physical safeguard standards for their electronic information systems whether such systems are housed on the covered entity’s premises or at another location.

6. **Question**: Does the HIPAA Security Rule allow for sending EPHI in an email or over the Internet? If so, what protections must be applied?

**Answer**: The HIPAA Security Rule does not expressly prohibit the use of email for sending EPHI. However, the standards for access control, (45 CFR § 164.312(a)) integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against the unauthorized access to EPHI. The standard for transmission security (§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect
EPHI as it is transmitted, select a solution, and document the decision. The Security Rule allows for EPHI to be sent over an electronic open network as long as it is adequately protected.

7. **Question:** Is mandatory encryption in the HIPAA Security Rule?

**Answer:** No. The final HIPAA Security Rule made the use of encryption an addressable implementation specification. See 45 CFR §§ 164.312(a)(2)(iv) and 164.312(e)(2)(ii). Covered entities use open networks such as the Internet and email systems differently, and no single interoperable encryption solution for communicating over open networks exists. Setting a single encryption standard could have placed an unfair financial and technical burden on some covered entities.

The encryption implementation specification is addressable, and must therefore be implemented if, after an assessment, the entity has determined that the specification is a reasonable and appropriate safeguard in its environment. If the entity decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate, or if the standard can otherwise be met, the covered entity may choose to not implement the implementation specification or any equivalent alternative measure.

8. **Question:** When do physicians have to have National Provider Identifiers?

**Answer:** Physicians can begin applying for National Provider Identifiers (NPIs) from the Centers for Medicare and Medicaid Services as of May 23, 2005. Physicians are not required to use NPIs until May 23, 2007. The single ID number will eventually replace all other identifiers that physicians use in reimbursement with private payers and the government.

**XIV. COMPUTERIZATION OF MEDICAL RECORDS AND SECURITY ISSUES**

**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.


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 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.

Obviously, 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 or valuable information which may impact the outcome of individual patient care.

Conversely, a central data base 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. CURRENT STATUS OF 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 patch-work 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 expected 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.


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.


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-3,290ee-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/admnsimp/nprm/). Administrative simplification includes standardizing electronic transactions and electronic signatures.

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 virtually no 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 or no 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 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 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 no 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.

XV. MEDICAL RECORDS AND LITIGATION

A. IMPORTANCE OF MAINTAINING GOOD/COMPLETE MEDICAL RECORDS

1. Improves patient care
2. Can substantiate a HCP=s position with respect to the care he/she provided
3. Failure to maintain such records could have negative consequences in litigation
   a. Michigan law basically provides that the absence of written records with respect to treatment can be create the presumption that such treatment was not provided.
   b. Could create a negative inference that the record, if it had existed, would have been detrimental to the HCP.
   c. Could give rise to spoliation of evidence claims.

B. PHYSICIAN/PATIENT PRIVILEGE

1. Statutory - MCLA '600.2157
   a. Waiver upon signing authorization
2. Exceptions
   a. Communications made in furtherance of unlawful or criminal purpose (i.e. testimony of physician relative to alterations in a prescription by patient charged with obtaining a controlled


d. Communications for the purpose of a lawsuit and not for treatment (i.e. results of blood test taken to disprove paternity - Osborn v Fabatz, 105 Mich App 450 (1981)).

e. Review of records by peer review organizations regarding services for which payment has been made under Title VIII of the Social Security Act.

f. Reports to state and federal agencies gathering health data (i.e. births, deaths, birth defects, AIDS, etc.).

g. Information released to a board or department acting within the scope of its authority regarding the licensure and regulation of health care professionals. MCLA '333.16244.

h. Reports of abuse of nursing home patients to the Department of Health. MCLA '333.21771.

i. Reports of suspected child abuse to the Department of Social Services. MCLA '722.625.

j. Reports of abuse of physically or mentally impaired adults to the Department of Social Services. MCLA '400.11a.

C. PSYCHOLOGIST AND PSYCHIATRIST/PATIENT PRIVILEGE

1. Statutory - MCLA '330.1750

2. Exceptions

   a. A communication shall be disclosed when it is relevant to a condition of the patient that the patient has introduced as an element of a claim or defense in a civil or administrative proceeding.
b. Communication disclosed when relevant to a matter under consideration in a proceeding governed by the Code if the patient was informed that the communication could be used in the proceeding.

c. In an action for malpractice.

d. Communication made during court-ordered examination, prior to which the patient was informed that it would not be privileged.

e. Communication made during treatment that the patient was ordered to undergo to render the patient competent to stand trial on a criminal charge.

D. SUBSEQUENT TREATING PHYSICIANS

In medical malpractice cases, non-party physicians treating the plaintiff subsequent to the alleged malpractice are frequently asked to produce records, testify in court, or meet with plaintiff or defense counsel.

1. Production of records
   a. Obtain authorization from patient
   b. Authorization by patient constitutes waiver of physician / patient privilege

2. Testimony in court / at deposition
   a. Subpoena required
   b. Authorization by patient required
   c. Produce records if requested
   d. May have personal or institutional attorney present

3. Interviews by attorneys

Ex parte contacts were recognized by the Michigan Supreme Court in Domako v Rowe, 438 Mich 347 (1991), and from that ruling it was concluded that where an attorney had received an authorization or there was a waiver of the privilege, that attorney could have ex parte meetings with the HCP without providing notice to the plaintiff.
With the passage of HIPAA and promulgation of the Privacy Rule, the continued permissibility of ex parte contacts appeared to meet its demise when the magistrate issued his opinion and order in Croskey v BMW of North America, et al. (02-73747). At issue was the plaintiff’s de bene esse deposition of one of the plaintiff’s treating physicians, and the defendants’ request for a protective order to meet ex parte with all of the plaintiff’s healthcare providers and treating physicians (the defendants apparently wanted to know what testimony would be provided at the deposition). The issue presented was whether ex parte contacts were viable in light of HIPAA and the Privacy Rule.

The magistrate looked at MCLA 600.2157 and interpreted it as forcing disclosure of medical information of a patient without a court order or the patient’s consent. He then contrasted this with the Privacy Rule under HIPAA and ruled that HIPAA permitted a compelled disclosure only via a court order or a subpoena containing certain assurances. Notwithstanding the fact that the plaintiff had signed an authorization, the magistrate concluded that HIPAA was more stringent than Michigan law because it gives the patient more control over his medical information and did not permit ex parte contacts. Accordingly, the defendant was required to: (1) give the plaintiff’s counsel notice; (2) obtain the plaintiff’s consent prior to any ex parte contacts; and (3) advise the plaintiff’s physicians that the interview is voluntary.

The magistrate’s order appeared to signal the end of ex parte meetings. However, the defendants filed objections, and in November 2005 the federal district court reversed the magistrate’s order. It concluded that the magistrate improperly grafted the requirements of notice and consent onto ex parte contacts, as nothing in the Privacy Rule explicitly mentioned ex parte contacts. The court further noted the possibility of HIPAA being used as both a sword and shield, which may run counter to Michigan law allowing for open and fair discovery with respect to a plaintiff’s physicians. The court, however, did agree with the magistrate that a physician must be advised as to both the purpose of the ex parte contact and that the physician is not required to grant the interview.

E.  MISSING RECORDS

Due diligence should be exercised in attempting to locate requested medical records. In the event records are missing, the requesting party should be promptly notified. The alteration or destruction of a medical record by an HCP for purposes of concealing responsibility for a patient=s injury is a felony. MCLA '750.429a.

F.  WHAT RECORDS MUST BE PRODUCED
A commonly asked question among HCPs is what medical records must be produced by the provider. Many providers take the position that only the records generated by that provider need be produced.

While there is no clear-cut answer, a recent legislative enactment would suggest that more than the provider’s own records must be produced. Effective April 1, 2004, PA 47, MCL 333.26.261 et seq., entitled The Medical Records Access Act of 2004, took effect. Among other things, this Act is designed to regulate access to and disclosure of medical records. It also defines medical records and healthcare providers, as well as establishes fees that may be charged for the production of medical records.

Many providers take the position that there was never a release from the other providers who generated the records. The Medical Records Access Act of 2004, however, defines "medical record" very broadly to include:

...information oral or recorded in any form or medium that pertains to a patient’s healthcare, medical history, diagnosis, prognosis, or medical condition and that is maintained by a healthcare provider or health facility in the process of the patient’s health (emphasis added).

With an appropriate authorization seeking "any and all medical records," it would appear that a physician is required to release the entire stack of records, even those produced by other care providers. Not only is the term "medical records" defined broadly, the language of the patient’s authorization that calls for the release of “any and all medical records” appears broad enough to encompass more than the provider’s own generated records.

G. VIOLATIONS OF HIPAA DURING DISCOVERY

As discussed above, HIPAA has impacted the ways litigants go about obtaining medical information about parties. However, what are the consequences if there is a violation of HIPAA during the course of litigation. This was the issue in Belote v. Strange, Case No. 262591 (October 25, 2005). There, the defendant obtained affidavits from the plaintiff’s prior treating physicians on an ex parte basis. In concluding that the meetings and resulting affidavit were improper under HIPAA, the court noted that HIPAA was more stringent than Michigan law since Michigan permitted ex parte meetings when there has been a waiver (however informal) of the physician-patient relationship. That is, HIPAA imposed requirements that Michigan law did not with respect to the disclosure of medical information.

Having found that there was a violation, the court nevertheless affirmed the trial court’s decision to allow the affidavits. It noted that a HIPAA violation would be treated as a discovery violation, and that the discovery violation
was outweighed by the concern that the patient had been less than truthful about her medical condition.

The conclusion that may be drawn from Belote is that violations of HIPAA do not necessarily render the evidence resulting from that violation inadmissible. Further, since the litigants in that case were not covered entities, they could not be subjected to HIPAA’s administrative penalties.

XVI. MINORS AND INCOMPETENT ADULTS

Several recent cases have outlined the law in situations where the durable power of attorney for health care is not applicable:

A. IN RE ROSEBUSH

In Re Rosebush, 195 Mich App 675 (1992). This case involved a request by the parents to remove respiratory life support for a 14 or 15 year old girl who was irreversibly paralyzed from the neck down due to a spinal cord injury and unable to breathe without a respirator. The desire of the parents to remove their daughter’s life support systems was blocked by the institution in which she was hospitalized and ultimately ended up in court. Important rulings from the case:

1. Michigan recognizes the common law right to be free from non-consensual physical invasions (informed consent).
2. A patient possesses the right not to consent i.e., the right to refuse treatment.
3. A competent adult patient has the right to decline any and all forms of medical intervention, including life saving or life prolonging treatment.
4. Because minors and incompetent patients lack the legal capacity to make decisions regarding their medical treatment, someone acting on their behalf must exercise their right to refuse treatment (substituted judgment) based on what the patient would have decided had he or she been competent. (Court said that a mature minor might prepare or make an advance medical directive and if he or she did so, that should be taken into consideration in deciding whether to terminate life support or nor.)
5. Parents (or guardians) are empowered to make decisions regarding withdrawal or withholding of life saving or life prolonging measures on behalf of their children.
6. In the case of an immature minor and others who were never competent, the *best interests* test is used. First, a court must look to evidence of the preference of the patient. Absent any evidence of the patient’s preference, a court must look to:

   a. evidence of the patient’s present level of physical, sensory, emotional and cognitive functioning;

   b. the degree of physical pain resulting from the medical condition from treatment and from termination of treatment;

   c. the degree of humiliation, dependence, and loss of dignity resulting from the condition and treatment;

   d. the life expectancy and prognosis for recovery, with and without treatment;

   e. the various treatment options; and

   f. the side effects and benefits of those options.

7. Some commentators have suggested that *In Re Rosebush* is authority for making living wills legally binding, based on the common law right to refuse medical treatment.

B. IN RE MARTIN

*In Re Martin*, 200 Mich App 703 (1993). This was a difficult case wherein the wife was appointed guardian of her husband and wanted to withdraw his nutritive support. However, this was opposed by his mother and his sister and the end decision ended up in court. Apparently, Michael Martin sustained a debilitating injury in an automobile accident, including a closed head injury, which significantly impaired his physical and cognitive abilities, leaving him unable to walk or talk and rendering him dependent on colostomy for defecation and gastrostomy for nutrition. Notably, the experts disagreed with Michael Martin’s level of physical, sensory incognitive functioning.

This court stated that it was the goal of the courts to effectuate a patient’s right of self-determination. Specifically, the court set forth the following tests in deciding whether or not to terminate life-supporting decisions:

1. Whether there is clear and convincing evidence of the patient’s previously expressed desires regarding life support under the conditions in which the court finds the patient to be.
2. If such evidence is not clear and convincing, the court may use the substituted judgment test as defined in Rosebush.

3. Only if the evidence in the first two categories does not yield a result may the court move on to consider a pure best interests standard. (Obviously, steps 2 and 3 also apply to minors and others who have never been competent.)

[200 Mich App at 713].

XVII. PATIENT SELF-DETERMINATION ACT

As noted above, the Patient Self-Determination Act enacted by Congress became effective December 1, 1991. This Act applies to all Medicare/Medicaid participating hospitals and its requirements are summarized as follows:

A. WHO MUST COMPLY WITH THIS LAW

The law applies to all of the following types of health care entities:

1. Hospitals;
2. Skilled nursing facilities;
3. Home health agencies;
4. Hospice programs;
5. HMOs / CMPs; and
6. Other prepaid organizations and comprehensive outpatient rehabilitation facilities.

B. WHAT MUST A HEALTH CARE ENTITY DO?

1. Written requirements

The above-referenced health care entities must provide all adult patients, residents or enrollees with written information regarding the following two (2) matters;

a. the individual=s right under the applicable state law to make health care decisions which includes the right to accept or reject medical or surgical treatment and the right to execute an advance directive; and
b. the policies of the health care entity respecting the implementation of such a right to accept or reject medical or surgical treatment.

2. Oral requirements

The health care entity must ask the individual upon admission if he or she has executed any form of an advance directive and to document that individual’s response in the patient or resident’s medical record.

3. Compliance with state laws

The health care entity is required to insure that the patient or resident has complied with the state legal requirements regarding advance directives (i.e. properly executed it and used the proper form).

4. Education

The health care entity is also required to educate its staff on advance directive issues. Notably, the law does not set forth what type of education will satisfy this requirement.

5. Withholding care

A health care entity may not condition its providing of health care to a patient based on whether that individual has or has not executed an advance directive. Similarly, a health care entity may not discriminate against an individual because he or she has or has not executed an advance directive.

6. Assistance

The law mandates that the Secretary of Health and Human Services shall assist each state with developing a special document which shall set forth an individual’s right to execute advance directives.

It is unclear what, if any, penalties apply to this section. Presumably, however, HCFA can withhold Medicare / Medicaid payments if a healthcare provider refuses to comply.

If you have any questions about the issues raised in these materials, please contact Mr. Christopherson at 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.