

Medical Information Privacy in Texas

Cynthia Marietta, J.D., LL.M.

Patricia Gray, J.D., LL.M.

UNIVERSITY of **HOUSTON** | LAW CENTER

Health Law & Policy Institute

Prepared for the Texas Health and Human Services Commission
and the Texas Health Services Authority with support from the State
Health Information Exchange Cooperative Agreement Program

TABLE OF CONTENTS

ACRONYMS	2
GLOSSARY	5
PREFACE	11
I. BACKGROUND ON PRIVACY OF MEDICAL INFORMATION	12
II. FEDERAL HIPAA PRIVACY PROTECTIONS	14
A. HIPAA APPLIES TO COVERED ENTITIES AND THEIR BUSINESS ASSOCIATES	15
B. HIPAA PROTECTS “PROTECTED HEALTH INFORMATION”	16
C. BASIC PRINCIPLE FOR USES AND DISCLOSURES OF PHI.....	18
D. LIMITING USES AND DISCLOSURES TO “MINIMUM NECESSARY” INFORMATION.....	25
E. NOTICE OF PRIVACY PRACTICES	26
F. INDIVIDUAL ACCESS TO REVIEW AND COPY RECORDS.....	26
G. ENFORCEMENT AND PENALTIES FOR NONCOMPLIANCE.....	29
III. FEDERAL HITECH PRIVACY PROTECTIONS	30
A. INDIVIDUALS’ RIGHTS TO ACCESS AND CONTROL OVER DISCLOSURES	30
B. BUSINESS ASSOCIATES SUBJECT TO COMPLIANCE.....	30
C. BREACH NOTIFICATION REQUIREMENTS.....	30
D. ACCOUNTING REQUIREMENTS FOR DISCLOSURES OF PHI IN EHRs.....	31
E. RESTRICTIONS ON MARKETING AND SALES OF PHI	31
F. ENHANCED ENFORCEMENT AND PENALTIES FOR NONCOMPLIANCE	32
IV. TEXAS MEDICAL RECORDS PRIVACY LAWS	34
A. LAWS RESTRICTING DISCLOSURE OF HEALTH INFORMATION	34
B. TEXAS CAUSES OF ACTION FOR UNAUTHORIZED DISCLOSURE OF PHI.....	43
V. TEXAS STATE LAW PREEMPTION	45
VI. CONCLUSION	46
END NOTES	47

ACRONYMS

AMA	American Medical Association
ARRA	American Recovery and Reinvestment Act of 2009, commonly referred to as the stimulus bill
CDC	Centers for Disease Control
CLIA	Clinical Laboratory Improvement Act
CMS	Center for Medicare and Medicaid Services
CPOE	Computerized Provider Order Entry
DSHS	Department of State Health Services
EEOC	Equal Employment Opportunity Commission
EPHI	Electronic Protected Health Information
FDA	Food and Drug Administration
FERPA	Family Educational Rights and Privacy Act
GINA	Genetic Information Nondiscrimination Act of 2008
GRC	Governance, Risk Management and Compliance
HHSC	Health & Human Services Commission
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act; statute includes direction to Federal Health & Human Services Commission to develop rules to protect health information privacy
HIT	Health Information Technology
HITECH	Health Information Technology for Economic and Clinical Health Act; incorporated into the federal stimulus legislation (ARRA)
HMO	Health Maintenance Organization
IIHI	Individually identifiable health information

IRB	Institutional Review Board
NCVHS	National Committee on Vital and Health Statistics
NHIN	National Health Information Network
NPRM	Notice of proposed rulemaking
OAG	Office of the Attorney General
OCR	Office of Civil Rights
OeHC	Office of e-Health Coordination
OIG	Office of the Inspector General
ONC	Office of the National Coordinator (for health information technology)
OSHA	Occupational Safety and Health Administration
REC	Regional Extension Center
PHI	Protected health information
RHIO	Regional Health Information Organization
THSA	Texas Health Services Authority
TMA	Texas Medical Association
TPA	Third party administrator
TPO	Treatment, payment, health care operations

FREQUENTLY REFERENCED CITATIONS

42 C. F. R. Part 2	Alcohol and Drug Abuse Confidentiality Requirements
Title II, Subtitle F, 42 USC 1320d et seq.	Health Information Portability and Accountability Act of 1996
21 CFR, Parts 50 and 56	FDA Protection of Human Subjects Regulations
20 USC 1232(g)	Family Educational Rights and Privacy Act
45 CFR Parts 160 and 164, Subparts A and E	HIPAA Privacy Regulations

GLOSSARY

Accounting for disclosures: *Report of information to an individual that describes a covered entity's disclosures of PHI other than for disclosures made for treatment, payment and health care operations or as part of a HIPAA compliant limited data set.*

Audit trail: *A record specifying the persons who have accessed an individual's PHI.*

Authentication: *Verification of the identity of an individual's or entity's right to access information in an individual's electronic health record.*

Authorization: *Permission from the individual or his or her personal representative to a provider to either obtain information about the individual from third parties or to release information about the individual to third parties for specified purposes.*

Business Associate: *Any individual or entity, other than a member of the covered entity's workforce, that is performing any activity or function on behalf of a covered entity involving the use or disclosure of PHI*

Business Associate Contract: *Required when a covered entity uses a contractor or other non-workforce member to perform business associate services or activities.*

Confidential: *Private and not intended for public disclosure*

Consent: *Frequently used interchangeability with authorization, but generally the written permission given by an authorized person that allows a provider or covered entity to disclose information about an individual.*

Covered entity: *Under HIPAA, health plans, health care clearinghouses and health care providers that transmit any health information in electronic form in connection with a transaction that is subject to HIPAA regulation. In Texas, covered entities include all persons and entities, their employees, agents, and contractors, who engage in the practice of assembling, collecting, analyzing, using, evaluating, storing or transmitting PHI, including all business associates, governmental units, and information management entities that possess or store PHI.*

Data use agreement: *Agreement between a researcher and a covered entity that limits the use of PHI that is part of a limited data set.*

De-identified health information: *Identifying information that has been deleted, redacted or blocked so that the remaining information neither identifies, nor provides a reasonable basis to identify the individual the subject of the information.*

Designated record set: *A group of records under the control of a covered entity from which information about the individual is retrieved in order to make decisions about the individual. Examples include health plan enrollment, payment and claims adjudication information, medical records and billing records.*

Direct treatment relationship: *The relationship between a health care provider and an individual that involves the direct provision of health care by the provider.*

Disclosure: *The release in any manner of information outside an entity holding the information. Disclosure is different from “use” which refers to the sharing of information within an entity.*

Electronic health record: *Information on a patient that conforms to nationally recognized interoperability standards. It can be created, managed and consulted by authorized clinicians and staff across more than one group.*

Electronic medical record: *Information on a patient that can be created, gathered, managed and consulted by authorized clinicians and staff in one health care organization*

Health care clearinghouse: *An information management entity that either processes or facilitates the processing of individually identifiable health information obtained from one entity for use by a receiving entity. Includes such entities as billing organizations, repricing companies, health information systems, and value added networks and switches.*

Health information exchange: *Electronic movement of health information among organizations according to nationally recognized standards.*

Health maintenance organization: *A managed care organization that provides health care through a network of physicians and other providers who agree to treat patients in accordance with the HMO guidelines in exchange for patients who contract only with that organization for health care services. Today HMOs are regulated for financial solvency as insurance plans are.*

Health care provider: *A person or entity that provides medical or health services as part of their normal business operations. Includes both institutional and non-institutional providers.*

Health care operations: *Administrative, financial, legal and quality improvement activities of a covered entity necessary to support the core functions of treatment and payment. Very broadly defined to incorporate almost all business related activities of a covered entity.*

Health plan: *For purposes of compliance with HIPAA, includes individual and group plans that provide or pay for the cost of any medical care, including health, dental, vision, and prescription drug insurers, HMOs, Medicare, Medicaid, Medicare+Choice and Medicare supplemental insurers, employer sponsored plans, long term care insurers, church sponsored plans and multi-employer plans..*

HIPAA: *A federal law defining the maintenance of health insurance eligibility for individuals changing employers or leaving the workforce. Incorporates regulatory authority for setting standards for electronic health care transactions (Administrative Simplification), federal health information privacy standards, and security requirements for the protection of health care information.*

HIPAA Privacy Rule: *The provisions developed under the federal rulemaking process to protect health information privacy.*

Hybrid entity: *A covered entity that performs business activities that include both covered and non-covered functions. Must designate its health care components for purposes of the Privacy Rule.*

Incidental disclosures: *Uses or disclosures of PHI that are accidental or unintentional and where the covered entity has used or disclosed the minimum necessary information and has safeguards in place to protect an individual's PHI.*

Indirect treatment relationship: *A relationship in which the health care services are furnished by a provider who does not deal directly with the patient, such as laboratory testing or analyzing diagnostic imaging results.*

Individually Identifiable Health Information: *Information related to an individual's health information that identifies the individual or that can reasonably be used to identify the individual.*

Institutional Review Board: *A reviewing entity for approval of research involving human subjects. Can waive or alter Privacy Rule requirements for an Authorization, but cannot waive or alter other human subject protections. Must be registered with the Office of Human Research Protection.*

Law enforcement purposes: *Six specific circumstances, subject to specific conditions, for which a covered entity may disclose PHI to law enforcement officials.*

Limited data set: *PHI for which certain specified identifiers of individuals have been removed. Data not fully de-identified. Used for research, health care operations, and public health purposes under data use agreements specifying permitted uses of safeguards for protection of the data.*

Marketing: *Includes communications by any means about products or services that encourage a recipient of the communication to buy or use the product or service. HIPAA excludes from the definition of marketing certain communication by a covered entity related to providers and plans participating in a network and the services or benefits covered by a health plan as well as communications related to care coordination or case management for treatment of an individual provided by the covered entity.*

Medicaid: *A joint federal-state program that provides health care insurance to low-income individuals.*

Medicare: *A federally funded program of outpatient and hospital insurance for persons aged 65 and older and for certain disabled persons. Prescription drug benefits were added in 2003.*

Medicare+Choice: *A type of Medicare plan that encompasses both Part A and Part B of Medicare as well as additional services such as vision, hearing, dental, and prescription drug coverage.*

Minimum necessary: *The least amount of information reasonably necessary to accomplish the intended purpose of the disclosure and use of the information.*

NCVHS: *A federal advisory entity charged with advising the Secretary of HHS about health information privacy and security.*

Notice of Privacy Practices: *A required notice to an individual of their rights concerning the uses and disclosures of the individual's PHI that may be made by a covered entity, and the covered entity's legal duties related to the individual's PHI.*

Payment: *Activities undertaken by or on behalf of a covered entity to fulfill responsibilities for coverage and provision of benefits under a health plan or to obtain reimbursement to a provider for the provision of health care.*

Permitted uses and disclosures: *A limited and specific activity for which a covered entity is permitted, but not required, to use or disclose PHI without an individual's authorization.*

Personal health record: *Information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources. It is controlled by the individual.*

Preemption: *The precedence of federal law over contrary state law. Based on the Supremacy Clause of the US Constitution (Article VI, Provision 2). In general, HIPAA defers to state law when the state law is more stringent than HIPAA.*

Privacy: *The right of an individual to control access to or disclosure of their PHI.*

Privileged: *Protected from disclosure under the law*

Protected Health Information: *Individually identifiable health information (IIHI), including demographic data about a patient, that relates to the individual's past, present or future physical or mental health, the provision of health care to the individual, and past, present or future payment for the provision of health care to the individual.*

Psychotherapy notes: *Information maintained by a mental health professional health care provider that document or analyze the content of a conversation in a counseling session, whether group or individual. Psychotherapy notes are kept separate from the rest of the individual's health record and do not include medication monitoring, diagnostic summaries, and progress notes. Currently under discussion are whether diagnostic test results should be included in the definition of psychotherapy notes. Use or disclosure of psychotherapy notes requires specific authorization from an individual except in limited, specified circumstances.*

Public health activities: *Specified activities for which covered entities may disclose PHI without patient authorization. Examples include information for public health authorities authorized by law to collect or receive information for the prevention and control of disease or injury, governmental entities authorized to receive reports of adult or child abuse or neglect, and workplace related illness or injury surveillance.*

Public Health Authority: *A public agency acting under a grant of authority to perform certain public health services or functions such as monitoring health status to identify community health problems, diagnosing and investigating health problems and health hazards in a community, and enforcing laws and regulations that protect public health and ensure safety.*

Re-disclosure: *The disclosure of information to a person or entity beyond the disclosure originally authorized or to a person or entity other than that originally authorized.*

Regional health information organization: *A body that brings together health care stakeholders within a defined geographic area and governs the exchange of health information among them according to nationally recognized standards.*

Required disclosures: *References two situations for which a covered entity is required to disclose PHI without prior authorization from the individual. The two situations requiring disclosure are (1) to the individual or his personal representative when they request access to or an accounting of disclosures of their PHI, and (2) to the federal HHSC when it is undertaking a compliance investigation, review or enforcement action.*

Required by law: *A requirement in law that compels disclosure of PHI by a covered entity without individual authorization, such as court orders, subpoenas or summons issued by a court or similar legal body compelling production of information, or an authorized investigative demand related to a criminal or civil investigations.*

Specially protected records: *Generally, records related to the treatment of mental illness or substance abuse, or certain diseases such as HIV or sexually transmitted diseases. Treatment for these conditions still carries a special stigma in the minds of many, and disclosure of an individual's tests for, test results or treatment generally requires specific authorization from the individual under both state and federal law.*

Standard: *A requirement delineating practices and procedures for the security and protection of an individual's PHI.*

Standard setting organizations: *An organization accredited by the American National Standards Institute (ANSI) that develops and maintains the requirements for information transactions or any other standard necessary to facilitate implementation of HIPAA privacy and security requirements.*

Third party administrator: *A third party administrator is an organization that manages functions such as claims processing for payment for a health care provider.*

Transaction: *The transmission of information between two parties to carry out financial or administration activities related to health care, including eligibility determination, coordination of benefits, payment, and claims' status.*

Treatment: *The provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.*

Use: *Sharing of information within the entity that maintains the information.*

PRIMER ON MEDICAL INFORMATION PRIVACY PROTECTIONS IN TEXAS

PREFACE

This Primer outlines pertinent federal and Texas laws and regulations that provide privacy protections for medical information. Federal protections are primarily found in various provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),¹ the HIPAA Privacy Rule² and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).³ The Texas protections are scattered throughout a number of state statutes and administrative regulations, including the Medical Practice Act⁴ and the Texas Medical Records Privacy Act.⁵ While the federal and Texas laws have some overlapping privacy protections, there are gaps as well. Moreover, HIPAA contains some express preemption provisions. The challenge is to reconcile and harmonize all overlaps, gaps and preemption provisions so that healthcare providers are enabled to obtain all necessary health information to effectively and appropriately treat their patients while ensuring that patients' medical records privacy rights are adequately protected.

This Primer focuses on the statutes referenced above and is not intended to be exhaustive of all privacy laws.

I. BACKGROUND ON PRIVACY OF MEDICAL INFORMATION

Physicians have an ethical duty to keep their patients' confidences.⁶ A physician's duty to maintain confidentiality means the physician may not disclose any medical information that he learns from or discovers about a patient in connection with treatment of that patient. According to the American Medical Association (AMA) Code of Medical Ethics,⁷ the information that a patient discloses to a physician during the course of the patient-physician relationship is considered confidential to the utmost degree.⁸

The purpose of a physician's ethical duty to maintain confidentiality is to encourage and allow the patient to freely disclose information to the physician with the understanding the physician will protect the confidential nature of the information disclosed.⁹ Full disclosure enables the physician to diagnose conditions properly and to treat the patient appropriately. In return for the patient's honesty, under the AMA's ethical guidelines the physician should not reveal confidential communications or information without the patient's express consent, or unless otherwise required by law to disclose the information.¹⁰

Maintaining patient confidentiality is not only an ethical duty, but is a legal duty as well. The Constitution of the United States, federal and state laws and regulations and the judicial system define this legal obligation. While the AMA's guidelines are not binding by law, courts nevertheless have used these ethical obligations as the basis for imposing legal obligations. Although the Constitution does not explicitly mention any right of privacy, the U.S. Supreme Court has recognized a right of personal privacy, or a protected "zone of privacy," in one's own medical information.¹¹ This privacy right is grounded in two different kinds of interests: one is the individual interest in avoiding disclosure of personal matters, and the other is the interest in independence in making certain kinds of important decisions, such as decisions about one's own health.¹² Having roots in the First, Fourth, Fifth, Ninth, and Fourteenth Amendments and the Bill of Rights, the right of privacy of medical information is not absolute, and may be subject to compelling state interests.¹³

Physicians and health-care providers are increasingly gaining access to confidential patient information through electronic health information systems. Generally, the information contained within a patient's medical record may be released to third parties, such as the patient's attorney, insurance company, employer, member of the patient's family, or governmental agencies, only if the patient expressly authorizes such disclosure.¹⁴

A breach of confidentiality occurs with disclosure of private medical information to a third party without patient consent, or court order, or the few other exceptions recognized under the law. Disclosure can be oral or written, by telephone, facsimile transmission or electronically by e-mail or health information networks. Courts generally allow a cause

of action for a breach of confidentiality against a treating physician who divulges confidential medical information without proper authorization from the patient. The legal basis for imposing penalties and liability for breach of confidentiality is derived from the patchwork of laws encompassing constitutional privacy rights and federal and state laws and regulations governing medical records designed to protect private and sensitive information.¹⁵

II. FEDERAL HIPAA PRIVACY PROTECTIONS

Congress enacted the Health Insurance Portability and Accountability Act of 1996 (the “HIPAA statute”)¹⁶ to improve the portability and continuity of health insurance coverage and establish standards for administrative simplification.¹⁷ The HIPAA statute directs the U.S. Department of Health and Human Services (HHS) to promulgate standards for the electronic exchange, privacy and security of health information. Pursuant to that directive, in 2002, HHS issued modified regulations, known as the HIPAA Privacy Rule, that establish national minimum standards for the protection of certain health information, known as Protected Health Information or “PHI.” The HIPAA Privacy Rule is often referred to as simply “HIPAA” or “Privacy Rule.”

The HIPAA Privacy Rule is the first federal legislation to initiate uniform privacy standards for patient information. Prior to the enactment of the Privacy Rule, it was left up to each state to provide legislation to protect the privacy of patient information. The Privacy Rule sets a floor of ground rules for health care providers, health plans, health care clearinghouses and their business associates that conduct certain health care transactions electronically to follow for protecting individuals’ medical records and other personal health information. Moreover, it creates a framework of protection that can be strengthened by both the federal government and by states as health information systems continue to evolve.¹⁸ HIPAA’s provisions allow existing state laws that are more protective of privacy to stand, and permit states to make more protective laws in the future.

The Privacy Rule requires appropriate safeguards to protect the privacy of individuals’ identifiable health information (PHI),¹⁹ and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.²⁰ Within HHS, the Office for Civil Rights (“OCR”) has responsibility for implementing and enforcing the Privacy Rule through voluntary compliance activities and civil money penalties.²¹

A major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information necessary to provide and promote high quality health care and to protect the public's health and well being.²² The Privacy Rule is intended to strike a balance that permits important uses of information while protecting the privacy of people who seek medical care.

Additionally, in 2003, HHS issued HIPAA Security regulations, known as the HIPAA “Security Rule,” which established minimum national standards to protect individuals’ electronic PHI that is created, received, used, or maintained by a covered entity and their business associates. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.²³

In 2009, Congress enacted HITECH, an integral component of the American Recovery and Reinvestment Act of 2009 (ARRA),²⁴ with the intent to create a national infrastructure for the exchange of health information. HITECH's privacy and security rules operate hand-in-hand with HIPAA, but provide broader individual rights and stronger protections in situations when third parties handle patients' PHI, including obligations to notify individuals and HHS in the event of certain breaches of the HIPAA Privacy Rule.²⁵ HITECH is further discussed in Section III below.

A. HIPAA Applies to Covered Entities and their Business Associates

The following "covered entities" must comply with the Privacy and Security Rules: health plans, health care clearinghouses, and any health care provider who transmits health information in electronic form in connection with transactions for which HHS has adopted standards under HIPAA. "Business associates" of these entities must comply as well. Covered entities must have a business associate agreement with their business associates to ensure compliance with safeguards for protecting patients' PHI.

Health Plans include individual and group plans that provide or pay the cost of medical care.²⁶ Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions, however; a group health plan with fewer than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) programs whose principal activity is directly providing health care, such as a community health center, or an entity that makes grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including those providing only workers' compensation, automobile insurance, and property and casualty insurance.²⁷

Health Care Providers include all providers of medical or health services, including institutional and non-institutional providers. This includes hospitals, physicians, dentists and other practitioners, and any other person or organization that furnishes, bills, or is paid for health care and who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule.²⁸ Simply using electronic technology, such as email, does not mean a health care provider is a covered entity. The transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf.²⁹ Practically speaking, virtually all health care providers are covered entities for purposes of the Privacy Rule.

Health Care Clearinghouses are entities that process nonstandard information they receive from another entity into a standard format or data content, or vice versa.³⁰ Health care clearinghouses include billing services, re-pricing companies, community health management information systems, and value-added networks and switches if these entities perform clearinghouse functions.³¹ In most instances, health care clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or health care provider as a business associate. In such instances, only certain provisions of the Privacy Rule are applicable to the health care clearinghouse's uses and disclosures of protected health information.³²

Business Associates include a person or organization, other than a member of a covered entity's workforce, who performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of PHI. Business associate functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.³³ Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.³⁴ However, persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all, such as janitorial services. A covered entity can be the business associate of another covered entity.³⁵

A Business Associate Agreement is required when a covered entity uses a contractor or other non-workforce member to perform "*business associate*" services or activities.³⁶ The Privacy Rule requires that a covered entity impose specified written safeguards on the PHI, including without limitation, electronic PHI used by, created by, or disclosed to or by its business associates. In certain circumstances, if a covered entity and its business associate are both governmental entities, they may use alternative means to achieve the same protections.³⁷ A covered entity may not contractually authorize its business associate to make any use or disclosure of PHI that would violate the Privacy Rule.³⁸

B. HIPAA Protects "Protected Health Information"

The Privacy Rule protects all "*individually identifiable health information*" or PHI held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.³⁹

Individually identifiable health information or PHI is information, including demographic data, which relates to:

- (1) The individual's past, present or future physical or mental health or condition;

- (2) The provision of health care to the individual;
- (3) The past, present, or future payment for the provision of health care to the individual; and
- (4) The identity of the individual or for which there is a reasonable basis to believe it can be used to identify the individual.⁴⁰

Individually identifiable health information includes many common identifiers, such as name, address, birth date, and Social Security Number.⁴¹

Consistent with the purpose of the Genetic Information Nondiscrimination Act of 2008 (GINA),⁴² the Office of Civil Rights within the U.S. Department of Health and Human Services issued proposed rules to modify the Privacy Rule to clarify that genetic information is health information protected by the Privacy Rule to the extent that it meets the definition of PHI. In other words, to be protected, the genetic information must be individually identifiable and maintained by a HIPAA covered entity or business associate of a covered entity and not otherwise fall within one of the exceptions to the definition of PHI.⁴³ The proposed rules would also modify the Privacy Rule to prohibit the use and disclosure of genetic information by covered health plans for underwriting purposes.⁴⁴

The Privacy Rule excludes from PHI any employment records that a covered entity maintains in its capacity as an employer and any education and other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

De-Identified Health Information neither identifies nor provides a reasonable basis for identification of an individual. When health information does not identify an individual, and there is no reasonable basis to believe that it can be used to identify an individual, then it is considered “de-identified” and not PHI.⁴⁵ The Privacy Rule designates two methods through which a covered entity or business associate can determine that health information is de-identified.⁴⁶ The first is the “safe harbor” method, which permits a covered entity to consider data to be de-identified if it removes 18 types of identifiers, such as names, dates, and addresses, and has no actual knowledge that the remaining information could be used to identify an individual, either alone or in combination with other information.⁴⁷ The alternative approach is the “statistical” method, which permits covered entities to disclose health information in any form provided that a qualified statistical or scientific expert concludes, through the use of accepted analytic techniques, that the risk the information could be used alone, or in combination with other reasonably available information, to identify the subject would be very small.⁴⁸ A covered entity may use or disclose de-identified health information for any purpose without restriction, unless other laws may apply and limit such use or disclosure.⁴⁹

C. Basic Principle for Uses and Disclosures of PHI

One major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by covered entities. A covered entity may not use or disclose PHI, except:

- (1) As the Privacy Rule *requires*;
- (2) As the Privacy Rule *permits*; or
- (3) As the individual who is the subject of the information (or the individual's personal representative) authorizes such use or disclosure in writing.⁵⁰

1. Required Disclosures Without Authorization:

A covered entity *is required to disclose PHI* in only two situations:

- (a) To individuals (or their legally authorized representative as defined by state law) when they request access to, or an accounting of, disclosures of their PHI, with some exceptions;⁵¹ and
- (b) To HHS when it is undertaking a compliance investigation or review or enforcement action.⁵²

2. Permitted Uses and Disclosures without Authorization:

A covered entity *is permitted, but not required, to use and disclose PHI*, without an individual's authorization for a variety of purposes, including but not limited to, the following purposes or situations:

- (a) To the individual with some exceptions (unless an authorization is required for access to or accounting of prior disclosures);
- (b) For treatment, payment, and health care operations;⁵³
- (c) To allow opportunity for the patient to agree or object to information in the patient's record;
- (d) When the use or disclosure is incidental to an otherwise permitted use and disclosure;
- (e) As required by law⁵⁴ discussed more fully below, including but not limited to, public health, health oversight, abuse, neglect or

domestic violence, judicial and administrative proceedings, law enforcement; and

- (f) As part of a Limited Data Set for the purposes of research, public health or health care operations.⁵⁵

An important exception to this permissive rule concerns the uses and disclosure of psychotherapy notes. A HIPAA compliant authorization is required when such psychotherapy notes are used for purposes of treatment, payment, or health care operations.⁵⁶

Covered entities may rely on professional ethics and best judgments in deciding which permissive uses and disclosures may be made without the individual's authorization.

- (a) To the Individual: A covered entity may disclose protected health information to the individual who is the subject of the information, with some exceptions.
- (b) Treatment, Payment, Health Care Operations: A covered entity *may use and disclose* PHI for its own treatment, payment, and health care operations activities.⁵⁷ A covered entity *also may disclose* PHI for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving quality or competency assurance activities, fraud and abuse detection, or compliance activities if both covered entities have or had a relationship with the individual and the PHI pertains to the relationship.⁵⁸

Treatment is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.⁵⁹

Payment encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.⁶⁰

Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance

programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information and creating a limited data set. In addition, health care operations may include certain fundraising activities for the benefit of the covered entity.⁶¹

Covered entities may opt to obtain “consent” (written permission) from individuals to use and disclose their PHI for treatment, payment, and health care operations. However, obtaining consent is optional under the Privacy Rule for all covered entities.⁶² A covered entity electing to use consent forms may use its own discretion in drafting the content of such a form and in the process used for obtaining consent.⁶³

(c) Uses and Disclosures with Opportunity to Agree or Object

Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures if, in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual. Typically, this applies in the following circumstances:⁶⁴

Facility Directories: It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual’s informal permission to list in its facility directory the individual’s name, general condition, religious affiliation, and location in the provider’s facility.⁶⁵

For Notification and Other Purposes: A covered entity also may rely on an individual’s informal permission to disclose to the individual’s family, relatives, friends, or to other persons whom the individual identifies protected health information directly relevant to that person’s involvement in the individual’s care or payment for care.⁶⁶ For example, this allows a pharmacist to dispense prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual’s informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual’s care of the individual’s location, general condition, or death. In addition, protected health information may be disclosed for notification

purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.⁶⁷

(d) Incidental Use and Disclosure: The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated.⁶⁸

(e) Public Interest and Benefit Activities: The Privacy Rule permits use and disclosure of PHI, without an individual's authorization or permission, for the twelve national priority purposes listed below.⁶⁹ These disclosures are permitted, although not required, in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information. Such public interest purposes include:⁷⁰

As Required by Law: Covered entities may use and disclose PHI without individual authorization for disclosures required by statute, regulation, or court orders.⁷¹

Public Health Activities: Covered entities may disclose PHI to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or similar state law.⁷²

Victims of Abuse, Neglect or Domestic Violence: In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.⁷³

Health Oversight Activities: Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.⁷⁴

Judicial and Administrative Proceedings: Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.⁷⁵

Law Enforcement Purposes: Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) in a medical emergency not occurring on the covered entity's premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, or the perpetrator of the crime.⁷⁶

Decedents: Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.⁷⁷

Cadaveric Organ, Eye, or Tissue Donation: Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.⁷⁸

Research: "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains:

- (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board;
- (2) representation from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for

similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or

(3) representation from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought. A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).⁷⁹

Serious Threat to Health or Safety: Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.⁸⁰

Essential Government Functions: An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.⁸¹

Workers' Compensation: Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.⁸²

(f) Limited Data Set:

A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed, leaving only indirect identifiers. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.⁸³

3. *Authorization Required for Uses and Disclosures:*

A covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or is otherwise permitted or required by the Privacy Rule.⁸⁴ A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances.⁸⁵

Under the Privacy Rule, an authorization must be written in specific terms. It may allow use and disclosure of PHI by the covered entity seeking the authorization or by a third party.⁸⁶ All authorizations must be in plain language and contain specific information regarding the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other data.⁸⁷

The Privacy Rule specifies two certain circumstances under which written authorization is required: use or disclosure of psychotherapy notes⁸⁸ and marketing,⁸⁹ but there are exceptions in each case.⁹⁰

(1) *Psychotherapy Notes:* A covered entity must obtain an individual's authorization to use or disclose psychotherapy notes,⁹¹ with the following exceptions:⁹²

- The covered entity who originated the notes may use them for treatment; and
- A covered entity may use or disclose, without an individual's authorization, the psychotherapy notes for its own training, to defend itself in legal proceedings brought by the individual, for HHS to investigate or determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.⁹³

(2) *Marketing:* Marketing is defined as any communication about a product or service that encourages recipients to purchase or use the product or service.⁹⁴ A covered entity must obtain an authorization to use or disclose protected health information for marketing, except for face-to-face marketing communications between a covered entity and an individual or for a covered entity's provision of promotional gifts of nominal value.⁹⁵ No authorization is needed, however, to make a communication that falls within one of the exceptions to the marketing definition.⁹⁶

Marketing is also defined as an arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services.⁹⁷ An authorization for marketing that involves the covered entity's receipt of direct or indirect remuneration from a third party must reveal that fact.⁹⁸

The HIPAA Marketing definitions and provisions were substantially revised in rule making, pursuant to HITECH. These revisions are discussed below in Section III.

D. Limiting Uses and Disclosures to “Minimum Necessary” Information

A central aspect of the Privacy Rule is the principle of “minimum necessary” use and disclosure. Other than what is specified in an authorization form and with few other exceptions, the Rule requires a covered entity to make reasonable efforts to use, disclose, and request only the minimum amount of protected health information necessary to accomplish the intended purpose of the use, disclosure, or request.⁹⁹

The Privacy Rule also requires a covered entity to develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. When the minimum necessary standard applies to a use or disclosure, a covered entity may not use, disclose, or request the entire medical record for a particular purpose unless it can specifically justify the whole record as the amount reasonably needed for the purpose.

Although the HITECH act, as discussed further below in Section III, requires HHS to promulgate new guidance on this “minimum necessary” standard, HHS has yet to do so.¹⁰⁰ HHS is currently seeking public comment on this issue and how the entities subject to the “minimum necessary” standard should determine what is necessary to comply with the Privacy Rule.¹⁰¹

The minimum necessary requirement is not imposed in any of the following circumstances:

- (a) Disclosure to or a request by a health care provider for treatment;
- (b) Disclosure to an individual who is the subject of the information, or the individual's personal representative;
- (c) Use or disclosure made pursuant to an authorization;

- (d) Disclosure to HHS for complaint investigation, compliance review or enforcement;
- (e) Use or disclosure that is required by law; or
- (f) Use or disclosure required for compliance with other HIPAA Rules.¹⁰²

Reasonable Reliance: If another covered entity makes a request for protected health information, a covered entity may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a covered entity may rely upon requests as being the minimum necessary protected health information from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the covered entity's business associate, seeking the information to provide services to or for the covered entity; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research.¹⁰³

E. Notice of Privacy Practices

The Privacy Rule requires that each covered entity, with certain exceptions, must provide a notice of its privacy practices and certain special statements.¹⁰⁴ The notice must contain certain elements. The notice must describe and in some cases provide at least one example of the ways in which the covered entity may use and disclose protected health information.

F. Individual Access to Review and Copy Records

Except in certain circumstances of restricted disclosure,¹⁰⁵ individuals have the right to review and obtain a copy of their protected health information in a covered entity's *designated record set*.¹⁰⁶ The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.¹⁰⁷ Exceptions to the right of access include psychotherapy notes, information compiled for legal proceedings, laboratory results to which the Clinical Laboratory Improvement Act (CLIA) prohibits access, or information held by certain research laboratories. For information included within the right of access, covered entities may deny an individual access in certain specified situations, such as when a health care professional believes access could cause harm to the individual or another. In such situations, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.¹⁰⁸ Covered entities may impose reasonable, cost-based fees to cover the costs of copying and postage.¹⁰⁹

1. Individual's Right to Amend their PHI:

The Privacy Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete.¹¹⁰ If a covered entity accepts an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it, and to persons that the covered entity knows might rely on the information to the individual's detriment.¹¹¹ If the request is denied, covered entities must provide the individual with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record. A covered entity must amend protected health information in its designated record set upon receipt of notice to amend from another covered entity.¹¹²

2. Right to Accounting of Disclosures:

Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.¹¹³ The maximum disclosure accounting period is the six years immediately preceding the accounting request, except that a covered entity is not obligated to account for any disclosure made before the date on which it was required to comply with the Privacy Rule.¹¹⁴

The Privacy Rule does not require accounting for disclosures:

- (a) For treatment, payment, or health care operations;
- (b) To the individual or the individual's personal representative;
- (c) For notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories;
- (d) Pursuant to an authorization;
- (e) Of a limited data set;
- (f) For national security or intelligence purposes;
- (g) To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or
- (h) Incidental to otherwise permitted or required uses or disclosures.¹¹⁵

Accounting for disclosures to health oversight agencies and law enforcement officials must be temporarily suspended on their written representation that an accounting would likely impede their activities.¹¹⁶

HITECH, as discussed further below, modifies the disclosure exemption noted above for disclosures made through electronic health care records (EHR) for purposes of treatment, payment, or health care operations. An “electronic health record” is “an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.”¹¹⁷

3. *Individuals’ Right to Restrict Use or Disclosures:*

Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual’s health care or payment for health care, or disclosure to notify family members or others about the individual’s general condition, location, or death.¹¹⁸ *A covered entity is under no obligation to agree to requests for restrictions with limited exceptions. A covered entity must agree to certain restrictions relating to disclosures to a health plan in certain circumstances¹¹⁹ and except for purposes of treating the individual in a medical emergency.¹²⁰*

As discussed further below in Section III, HITECH strengthens individuals’ control over and access to their PHI.

4. *Personal Representatives:*

The Privacy Rule requires a covered entity to treat an individual’s “*personal representative*” if under the applicable law the personal representative has authority to act on behalf of the individual¹²¹ the same as the individual with respect to uses and disclosures of the individual’s protected health information and with regard to the individual’s rights under the Rule.¹²² A personal representative is a person legally authorized to make health care decisions on an individual’s behalf or to act for a deceased individual or the person’s estate. In these situations, the Privacy Rule defers to state and other law to determine the rights of personal representatives. Texas provides for a variety of “legally authorized representatives.”¹²³ The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.¹²⁴

5. *Minors:*

In most cases, parents are the personal representatives for

their minor children. Therefore, in most, but not all cases, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. In certain exceptional cases, the parent is not considered the personal representative. In these situations, the Privacy Rule defers to state and other law to determine the rights of parents to access and control the protected health information of their minor children. If State and other law is silent concerning parental access to the minor's protected health information, a covered entity has discretion to provide or deny a parent access to the minor's health information, provided that the decision is made by a licensed health care professional in the exercise of professional judgment.¹²⁵

G. Enforcement and Penalties for Noncompliance

The Privacy Rule provides processes for persons to file complaints with HHS concerning PHI use and disclosure violations and describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews.¹²⁶

As discussed in Section III below, HITECH enhances enforcement of HIPAA by adding new enforcement provisions, including a tiered system for imposing civil monetary penalties for HIPAA violations and empowering state attorneys general to bring civil suits to enforce HIPAA.¹²⁷

III. FEDERAL HITECH PRIVACY AND SECURITY PROTECTIONS

In 2009, Congress enacted HITECH, an integral component of the American Recovery and Reinvestment Act of 2009 (ARRA),¹²⁸ with the intent to create a national infrastructure for the exchange of health information. HITECH's privacy and security rules build on and strengthen federal health information privacy laws, and in particular the HIPAA Privacy Rule. HITECH serves to broaden HIPAA's reach, strengthen its privacy and security standards and expand its enforcement provisions.¹²⁹ HITECH outlines a detailed timeline for implementation of its privacy provisions, and as consistent with HITECH's requirements, HHS and other designated agencies have issued requisite reports, proposed rules, and policy guidance for purposes of implementing the privacy rules.¹³⁰

Some of HITECH's most significant provisions that concern privacy and security include the following:

A. Individuals' Rights to Access and Control over Disclosures

HITECH enhances an individual's control over and access to PHI. By way of example, a covered entity must comply with an individual's request to restrict disclosure of PHI to a health plan for purposes of payment or health care operations if the PHI pertains to a procedure or service that was paid out of pocket in full.¹³¹ In cases when a covered entity uses EHR containing PHI, the individual has a right to obtain a copy of the record in electronic format and may direct the covered entity to transmit such copy to a designated entity or person.¹³²

B. Business Associates Subject to Compliance

HITECH extends the reach of government enforcement beyond covered entities to their business associates,¹³³ by making the business associates directly responsible for compliance with the new HITECH privacy provisions, portions of the HIPAA Security Rule, and all provisions in their business associate agreements.¹³⁴ HITECH also clarifies which certain entities are considered business associates and requires health information exchanges (HIE) and other organizations that transmit PHI or have routine access to PHI to be treated as business associates that must enter into business associate agreements.¹³⁵

C. Breach Notification Requirements

HITECH creates notification requirements for covered entities, business associates, vendors of personal health records, and non-HIPAA covered entities in the event of a breach of unsecured PHI.¹³⁶ These requirements specify the methods of notice to be used, content of notice, timeline limitations, and record-keeping of such breaches.¹³⁷ In August 2009, the Office of Civil Rights (OCR) within HHS issued an Interim Final Rule implementing breach notification requirements for covered

entities.¹³⁸ The Federal Trade Commission issued similar requirements for PHR vendors not covered by HIPAA.¹³⁹ HHS' Interim Final Rule became effective September 23, 2009, with enforcement of the law effective February 22, 2010. The Interim Final Rule will remain in effect until HHS finalizes the rule. Any time after February 2011, changes are expected to HHS' breach notification requirements, following withdrawal of the interim regulations in August 2010.¹⁴⁰

D. Accounting Requirements for Disclosures of PHI in EHRs

HITECH modifies the exception noted above for treatment, payment, or health care operations, as it pertains to electronic health care records (EHR).¹⁴¹ HITECH provides that, if disclosures are made "through an electronic health record" for purposes of carrying out treatment, payment, and health care operations, then under HITECH, an individual has a right to receive an accounting of such disclosures that covers disclosures made during the three years prior to the request.¹⁴² This requirement raised concerns about how covered entities would balance the interests of individuals in learning the circumstances under which their PHI is being disclosed and the administrative burden of accounting for disclosures for treatment, payment, and health care operations through an electronic health record.¹⁴³ Due to these concerns, HHS has requested public comment before it publishes the necessary guidance for covered entities on this disclosure issue.¹⁴⁴

E. Restrictions on Marketing and Sales of PHI

HITECH places new restrictions on the marketing and sales of PHI. Patient consent is required for marketing communications unless they describe a drug or biologic currently prescribed for the patient.¹⁴⁵ Covered entities and business associates are prohibited from selling PHI without specific authorization, with a few noted exceptions, such as for public health activities, research and population registries.¹⁴⁶

Pursuant to rulemaking following the enactment of HITECH, marketing has been redefined to mean:

- (1) Except as provided in paragraph (2) of this definition, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.
- (2) Marketing does not include a communication made:
 - (i) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual, provided, however, that if the communication is in writing and the health care provider receives financial remuneration in exchange for making the communication, the requirements of § 164.514(f)(2) are met.

(ii) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication.

(iii) For the following health care operations activities, except where the covered entity receives financial remuneration in exchange for making the communication:

(A) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

(B) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(3) Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.¹⁴⁷

F. Enhanced Enforcement and Penalties for Noncompliance

HITECH enhances enforcement of HIPAA by adding new enforcement provisions, including a tiered system for imposing civil monetary penalties for HIPAA violations and empowering state attorneys general to bring civil suits to enforce HIPAA.¹⁴⁸ The tiered system is based on the violator's level of cognizance with respect to each violation and takes into account the harm done by the violation, as well as the nature and the extent of the violation.¹⁴⁹ The lowest penalties are assigned where there was no knowledge of the violation, and the highest where there was an element of "willful neglect." The penalties range from \$100 - \$50,000 per violation, with a maximum penalty imposed in the amount of \$1.5 million.

If the attorney general of a state has reason to believe that the interest of one or more residents of that state has been or is threatened or adversely affected by any person who violates HITECH and the Privacy Rule, then the attorney general may bring a civil

suit on behalf of the residents in state district court and seek injunctive relief and monetary damages.¹⁵⁰

Covered entities and business associates will be subject to periodic audits to ensure they comply with HITECH and the Privacy Rule.¹⁵¹ When PHI is maintained by covered entities and business associates, employees of such covered entities and business associates or other individuals may be subject to criminal penalties for wrongfully obtaining or disclosing the PHI without authorization.¹⁵²

IV. TEXAS MEDICAL RECORDS PRIVACY LAWS

In addition to HIPAA and HITECH, there other federal laws and Texas laws that address the privacy of medical records, in general, and more specifically, the privacy of certain records that have been regarded by some entities as “sensitive health information” (SHI). Although there has been considerable debate as to what constitutes SHI and whether it should be defined as a category distinct from other types of health information, SHI is generally considered to be information that carries with it unusually high risks in the event of disclosure.¹⁵³ The sensitivity of data is often influenced by the context in which it appears.¹⁵⁴ Categories of health information often considered to be “sensitive” include information related to minors, domestic violence, genetics, mental health, reproductive care and health, substance abuse, or sexually transmitted diseases, including HIV/AIDS.¹⁵⁵

A. *Laws Restricting Disclosure of Health Information*

In Texas, state-based restrictions on disclosures of private health information, including SHI, are primarily scattered throughout the following statutes and regulations and often are required by or mirror federal requirements:

1. *Physician-Patient Communications Privilege:*

The most widely recognized set of restrictions on disclosures of health information is found within the Texas Medical Practice Act as it pertains to physician-patient communications.¹⁵⁶ In Texas, all communications between a physician and patient related to, or in connection with, the physician’s professional services rendered to the patient are considered confidential and privileged.¹⁵⁷ Moreover, the patient’s medical information and records created and maintained by the physician are confidential and privileged.¹⁵⁸ This information is confidential, meaning that is private and not intended for public disclosure.¹⁵⁹ It is privileged in the sense that it is protected from disclosure under the law.¹⁶⁰

Maintaining the confidentiality of patient records is part of the core function of the provision of health care services.¹⁶¹ The patient's records reflect and memorialize the services that were rendered.¹⁶² The privilege between a physician and his patient is an expression of the standard in the health care profession which recognizes the confidential nature of the scope of the relationship and the communications that occur within the context of that relationship.¹⁶³

Section 159.002 of the Texas Occupations Code expressly prohibits a physician from disclosing to third parties all communications he has with a patient and the medical records he creates or maintains on that patient unless he has the patient’s *written* consent to do so.¹⁶⁴ The medical records protected under this privilege include all recorded or documented communications between the patient and the physician and the identity,

evaluation, diagnosis, and treatment of the patient.¹⁶⁵ This privilege of confidentiality may be claimed by the patient or by the physician.¹⁶⁶ The physician may claim the privilege of confidentiality on behalf of the patient, and the physician's authority to do so is presumed in the absence of evidence to the contrary.¹⁶⁷ The privilege applies regardless of when the physician treated the patient, except for medical records that are at least 100 years old and that are being reviewed for historical research purposes only.¹⁶⁸

There are a number of exceptions to this privilege. A patient's medical records may be disclosed in a court or administrative proceeding without the patient's consent.¹⁶⁹ Further, disclosures may be made without consent to a governmental agency, or as required or authorized by law.¹⁷⁰ Disclosures may also be made to qualified personnel for research, a management audit, a financial audit, or a program evaluation, but such personnel may not identify a patient in any report used in the research, audit, or program evaluation, or otherwise disclose the patient's identity.¹⁷¹

The purpose for the physician-patient communications privilege is two-fold: (1) to encourage the full communication necessary for effective evaluation and treatment, and (2) to prevent unnecessary disclosure of highly personal information.¹⁷² The first purpose is apparent -- to allow for complete communication without fear of disclosure so the physician can effectively render services.¹⁷³ The latter purpose reflects an understandable desire to maintain privacy.¹⁷⁴

Under TEX. OCC. CODE § 159.005(a), a physician is permitted to disclose confidential medical records and patient communications if the patient or the patient's legal representative provides written consent for the release of the confidential information.¹⁷⁵ The written consent must be signed by the patient or his designated representative and must specify:

- (1) the medical records to be covered by the release,
- (2) the reasons or purposes for the release; and
- (3) the person to whom the information is to be released.¹⁷⁶

Sections 159.005(c) and (d) allow the patient or his authorized representative to withdraw the consent to the release of the information, but notice of withdrawal of the consent must be in writing to have legal effect.¹⁷⁷ A third party who receives confidential information pursuant to written consent may disclose the confidential information, but only to the extent consistent with the authorized purpose for which the consent to release the information was originally obtained.¹⁷⁸ This confidentiality law prohibits the unauthorized disclosure of medical information by the person who initially obtained the information through consent.¹⁷⁹

Texas appellate courts have recognized that medical records do not lose their confidential status simply because a patient's identifying information is redacted. In other words, redaction of identifying information from medical records does not defeat the medical records privilege.¹⁸⁰ This is because redaction of identifying information does not address the concerns about confidential portions of the medical records relating to

diagnosis, evaluation, and treatment.¹⁸¹ Redacted medical records may not be disclosed without a patient's written consent.¹⁸²

Likewise, re-identified medical records may not be disclosed without a patient's consent. The Texas Legislature has specifically addressed the issue of disclosing re-identified protected health information, providing:

A person may not re-identify or attempt to re-identify an individual who is the subject of any protected health information without obtaining an individual's consent or authorization if required under this chapter or other state or federal law.¹⁸³

Thus, a patient must give the proper written consent for the release of his medical records regardless of whether his identifying information has been redacted or re-identified.

Notwithstanding the physician-patient communications statutory privilege, Texas courts and the Texas Attorney General's office have concluded that an individual's medical records fall within the zone of privacy protected by the U. S. Constitution.¹⁸⁴ While neither the U.S. Constitution nor the Texas Constitution expressly mentions any right of privacy in medical records, the U.S. Supreme Court recognized a right of personal privacy, or protected zone of privacy, in one's own medical information and the right to prevent unlimited disclosure of such personal information.¹⁸⁵

2. *Other Professional Health Care Provider-Patient Confidential Communications Privilege:*

Various Texas state statutes concerning other professional health care providers recognize privileged health care provider-patient communications similar to the physician-patient communications privilege. These statutes require written patient consent for disclosure, but also allow for some exceptions. Professional non-physician health care providers subject to the confidential communications privilege include, but are not limited to, chiropractors, podiatrists, and dentists.¹⁸⁶ Not all statutes concerning licensed health care providers were reviewed for purposes of this Primer, but each licensed health care provider in Texas is subject to some form of a health care provider-patient confidential communications privilege.

3. *Texas Medical Records Privacy Act:*

The Texas Medical Records Privacy Act (TMPRA), found in TEX. HEALTH & SAFETY CODE §§ 181.001- .205, was enacted in 2001 and incorporates and expands the protections mandated by HIPAA. The TMRPA is an example of a state law that provides more protection for patient privacy than is provided under the original HIPAA Privacy Rules. It incorporated the basic tenets of the HIPAA Privacy Rule while providing additional protections for Texas residents in areas where HIPAA, as originally passed,

left gaps. HITECH has closed some of those gaps with respect to restrictions on the marketing and sales of PHI.

The TMRPA expands HIPAA privacy protections in essentially two areas. First, the TMRPA applies to a broader range of covered entities that include all persons and entities, and their employees, agents, and contractors, who engage in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI.¹⁸⁷ Covered entities include all business associates, health care payers, governmental units, information or computer management entities, schools, health researchers, health care facilities, clinics, health care providers, and persons maintaining internet sites that possess, obtain or store PHI.¹⁸⁸ Second, the TMRPA prohibits a person from re-identifying or attempting to re-identify an individual who is the subject of any PHI without obtaining the individual's consent or authorization if required under the TMRPA, HIPAA, or any other state or federal law.¹⁸⁹

4. Health Care Facilities' Restrictions on Disclosure of Records:

Various Texas statutes address confidentiality requirements and impose restrictions on the disclosure of patient records in a variety of health care facilities. Separate statutes address confidentiality requirements for patient records in hospital settings,¹⁹⁰ nursing care facilities,¹⁹¹ intermediate care facilities,¹⁹² ambulatory surgery centers,¹⁹³ and free-standing emergency centers.¹⁹⁴ For instance, a patient's health care information may be disclosed without the patient's written authorization in a hospital setting under the following circumstances:

- (1) When the disclosure is for directory information, unless the patient expressly requests no disclosure or the directory information is otherwise protected by state or federal law;
- (2) To an employee or agent of the hospital who needs such information for health care education, quality assurance, peer review, or for assisting the hospital in the delivery of health care or in complying with statutory, licensing, accreditation, or certification requirements;
- (3) To a federal, state, or local governmental agency or authority to the extent authorized or required by law;
- (4) For use in a research project authorized by an institutional review board under federal law;
- (5) For a health maintenance organization for purposes of maintaining a statistical reporting system as required by law.¹⁹⁵

5. *Mental Health Records:*

Licensed and authorized professionals who treat mental health patients are subject to the mental health professional-patient communications privilege, which is similar in scope to the physician-patient communications statutory privilege. Chapter 611 of the Texas Health and Safety Code addresses the confidential nature of mental health records.¹⁹⁶ Communications between mental health professionals and their patients are confidential and privileged and are prohibited from disclosure to third parties unless an exception applies.¹⁹⁷ Moreover, the medical records the mental health professional creates and maintains are likewise confidential and privileged, with few exceptions.¹⁹⁸ *Thapar v. Zezulka*, 994 S.W.2d 635, 638 (Tex.1999) (confirming the confidential nature of communications between patients and mental health professionals and the prohibition against disclosure of records and communications unless an exception applies). Written patient consent is required for disclosure, with certain other exceptions.¹⁹⁹ Physicians may withhold their psychotherapy notes from a patient if the physician feels such disclosure to the patient is not in the patient's best interest.²⁰⁰

Moreover, there are statutory privacy protections for the records of individuals receiving services for intellectual disabilities (formerly persons with mental retardation) scattered throughout the Texas Health and Safety Code,²⁰¹ as well as referenced in the federal Family Educational Rights and Privacy Act (FERPA)²⁰² and the federal and Texas protection and advocacy statutes,²⁰³ as discussed further below.

6. *HIV/AIDS Records:*

Both the Texas Health & Safety Code § 81.103 and the Texas Insurance Code § 545.057 generally address the confidential nature of HIV-related test results.²⁰⁴ Persons who have knowledge or possess a test result may not release or allow the test result to become known except as required by law or by the individual's authorization.²⁰⁵ Criminal penalties and civil remedies may result in the event of unlawful disclosure.²⁰⁶ Any statement that an identifiable individual has or has not been tested with a home collection kit for HIV- infection testing, including a statement or assertion that the individual is positive, is negative, or is at risk, or has or does not have a certain level of antigen or antibody, is confidential.²⁰⁷

The Texas Department of Criminal Justice (TDCJ) is required to maintain confidentiality of test results of an inmate indicating HIV infection at all times, including after the inmate's discharge, release from state jail, or release on parole or mandatory supervision.²⁰⁸

Further, each Texas state agency is required to develop and implement guidelines regarding confidentiality of AIDS and HIV- related medical information of employees of the agency and for clients, inmates, patients, and residents served by the agency. Each

entity that receives funds from a state agency for residential or direct client services or programs must develop and implement guidelines regarding confidentiality of AIDS and HIV-related medical information for employees of the entity and for clients, inmates, patients and residents served by the entity. The confidentiality guidelines should be consistent with guidelines published by the Texas Department of State Health Services (DSHS) and with state and federal law and regulations.²⁰⁹

7. *Communicable Disease Information:*

Texas Health & Safety Code § 81.046 addresses the confidential nature of test results for communicable diseases. The result of a test for a communicable disease is confidential, and any person who possess or has knowledge of a test result may not release or disclose the test result or allow the test result to become known, with few exceptions.²¹⁰ A person may release or disclose a test result for statistical summary purposes without the written consent of the person tested if identifiable information is removed from the report.²¹¹

Reports, records, and information received from any source furnished to a public health district, health authority, local health department or DSHS that relate to cases or suspected cases of diseases or health conditions are confidential and are not public information and may not be released to the public.²¹² Subject to certain confidentiality requirements, DSHS shall require reports of disease outbreaks and individual cases known to be of importance to the general public and shall evaluate those reports to determine trends and nature and magnitude of hazards. DSHS may not include any identifiable information in any analysis or report.²¹³

Medical and epidemiology information may be released for statistical purposes: (1) if released in a manner without providing identifiable information, (2) if the appropriate state agencies comply with the requisite rules relating to the control and treatment of communicable diseases and health conditions or under other federal and state laws that expressly authorize disclosure, and (3) to appropriate federal agencies, such as the Centers for Disease and Control and Prevention (CDC) as long as the information is limited to name, address, sex, race, occupation, date of disease onset, source of infection, and other requested information relating to the case or suspected case of communicable disease.²¹⁴

8. *Genetic Information:*

Both the Texas Occupations Code §§ 58.102 - .104 and the federal Genetic Information Non-Discrimination Act of 2008 (GINA)²¹⁵ address the confidential nature of genetic information. Genetic information is considered confidential and privileged and requires authorization for disclosure, with few exceptions.²¹⁶ It may be disclosed without the individual's authorization under certain circumstances, if: (1) required by state or

federal court order, (2) authorized by state or federal criminal law, (3) used to establish paternity, (4) used to identify a decedent, (5) used for medical diagnostic purposes, or (6) the disclosure is for information from a research study which complies with all national standards for protecting human research subjects in obtaining informed consent, including Food and Drug Administration regulations (21 C.F.R. Part 50) and the federal common rule for Human Subject Research Protections (45 C.F.R. Part 46), the information does not identify a specific individual, and the information is provided to DSHS to comply with Chapter 87 of the Health & Safety Code.²¹⁷

9. *Substance Abuse:*

Various provisions scattered throughout the Texas Health and Safety Code,²¹⁸ Texas Administrative Code²¹⁹ and in the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations²²⁰ protect the confidential nature of alcohol and substance abuse patient treatment records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program.²²¹ Generally, and with limited exceptions, such substance abuse patients must give written consent for disclosure of their treatment records.²²²

10. *Records Used for Morbidity and Mortality Studies:*

Texas Health & Safety Code §§ 161.0213 and 161.022 address the confidential nature of identifiable morbidity and mortality reports. Medical care providers may provide interviews, reports, statements, memoranda, or other information relating to the condition and treatment of any person to be used in a study to reduce morbidity or mortality or to identify persons who may need immunization to the DSHS.²²³ The identity of a person whose condition or treatment has been studied is confidential and may not be revealed except in immunization surveys conducted for the department to identify persons who need immunization.²²⁴

11. *Public Health Records:*

Reports, records, and information furnished to the Commissioner of Public Health or the Texas Commission on Environmental Quality that relate to an epidemiology or toxicology investigation of human illnesses or conditions or environmental exposures that are harmful or believed to be harmful to the public health are not public information and are confidential.²²⁵

12. *Reporting of Occupational Conditions:*

Certain medical professionals are required to report suspected cases of work-related disease or health conditions to DSHS.²²⁶ All information and records related to the reportable condition are confidential, and may not be released or made public on

subpoena or otherwise.²²⁷ Such information may be released for statistical purposes, but without identifiable information.²²⁸

13. *Minors:*

Numerous Texas statutes outline the confidential nature of health records of minors, in general, and including those minors who are in foster care, are under Child Protective Services, exhibit mental health and intellectual disabilities, or are offenders in state custody.²²⁹ Various restrictions are placed on disclosure of minors' records.

14. *Inmate Records:*

The health care information of a defendant or an inmate confined in a facility operated by or under contract with the TDCJ may be exchanged between TDCJ health care personnel and health care personnel of the University of Texas Medical Branch at Galveston or Texas Tech University Health Sciences Center without the defendant's or inmate's authorization.²³⁰

15. *School Records:*

Generally, schools may maintain health records from other entities and must have written permission from the parent or eligible student in order to release any information from a student's education record. However, the Family Educational Rights and Privacy Act (FERPA)²³¹ allows schools to disclose those records, without consent, to certain parties and under certain conditions.²³² Texas regulates the disclosure of educational records of individuals receiving services for intellectual disabilities (formerly mental retardation).²³³

16. *Biometric Identifiers:*

A "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.²³⁴ In Texas, a governmental body that possesses a biometric identifier of an individual may not sell, lease, or otherwise disclose the biometric identifier to another person unless the individual consents to the disclosure; the disclosure is required or permitted by federal or Texas law; or the disclosure is made by or to a law enforcement agency for a law enforcement purpose.²³⁵ The governmental body must store, transmit, and protect biometric identifier from disclosure using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental body stores, transmits, and protects its other confidential information.²³⁶ Biometric identifiers in the possession of a Texas governmental body are exempt from disclosure under the Texas Open Records Act, Chapter 552 of the Texas Government Code.²³⁷

17. Medicaid Beneficiaries:

Federal and Texas statutes and regulations govern the extensive restrictions placed on Texas state agencies' use and disclosure of information, including health information, concerning Medicaid applicants and participants.²³⁸ For example, Texas must safeguard and restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan; and at Texas' option, the exchange of information necessary to verify the certification of eligibility of children for free or reduced price breakfasts under the Child Nutrition Act of 1966²³⁹ and free or reduced price lunches under the Richard B. Russell National School Lunch Act,²⁴⁰ in accordance with section 9(b) of that Act,²⁴¹ using data standards and formats established by Texas.

18. State Children's Health Insurance Program (SCHIP) Beneficiaries:

Like Medicaid, SCHIP²⁴² programs must restrict the use or disclosure of information concerning applicants and recipients to purposes directly related to plan administration.²⁴³ SCHIP is the federal/Texas partnership similar to Medicaid, that expands health insurance to targeted, low-income, uninsured children with family incomes too high to qualify for Medicaid, but who cannot afford private insurance.

19. Texas Protection and Advocacy System Clients:

The Texas protection and advocacy program, Texas Advocacy, Inc., was mandated and established pursuant to three federal statutes:²⁴⁴ the Developmental Disabilities and Bill of Rights Act (the DD Act),²⁴⁵ the Protection and Advocacy for Mentally Ill Individuals Act of 1986 (the PAIMI Act),²⁴⁶ and the Protection and Advocacy of Individual Rights Act (the PAIR Act),²⁴⁷ collectively "the federal protection and advocacy statutes." The statutes specifically authorize state protection and advocacy systems to investigate incidents of abuse or neglect of individuals when there is probable cause to believe an individual has been, or may be, subject to abuse or neglect.²⁴⁸ Such systems may also pursue administrative, legal and other appropriate remedies to ensure the protection of individuals with disabilities or mental illness in the state.²⁴⁹ The Texas Advocacy, Inc. program has broad investigatory authority, including authority to access to certain records of individuals who fall within the protection of the program,²⁵⁰ but the program can only access an individual's records if such individual or legal guardian, conservator, or other legal representative of such individual, has authorized the program to have such access, with limited exceptions."²⁵¹

20. Texas Breach Notification Statutes:

Chapter 2054.1125 of the Texas Government Code requires certain businesses and state agencies to comply with certain provisions within the Texas Business and Commerce Code that govern the handling of "sensitive personal information" (SPI) that

collected or maintained by the business in the regular course of business.²⁵² Such businesses and agencies must implement reasonable procedures: (1) to protect from unlawful use or disclosure any SPI; (2) to set standards for destruction of SPI; and (3) to provide notification in the event of a breach of system security and unauthorized acquisition of computerized data that would compromise the security, confidentiality, or integrity of SPI.²⁵³ Notification may be delayed under certain circumstances.²⁵⁴

21. *Texas Government Records:*

The Texas Open Records Act provides that all information, in any form, that is collected, assembled, or maintained by governmental bodies and agencies operating in whole or in part with state funds and in connection with official business transactions is considered public information.²⁵⁵ There are certain exceptions to the Texas Open Records Act, however. One such exception is information that is deemed confidential by law, such as PHI.

22. *Health Records Made Subject of Peer Review Committee Investigation:*

In Texas, a medical peer review committee is defined as a committee or professional review body that operates pursuant to written bylaws or protocol, as approved by or formed by the governing body, policy-making body or medical staff of an entity, for the purpose of monitoring the competency of health care practitioners and/or the quality of care delivered to patients.²⁵⁶ All patient medical records that are compiled, reviewed, and made the subject of deliberation in connection with confidential peer review investigations and proceedings are privileged from disclosure, with limited exceptions.²⁵⁷ Such records may be shared with and disclosed to governmental agencies, state medical boards, and other peer review bodies, but are not subject to public disclosure, absent court order or written waiver executed by the committee.²⁵⁸

B. *Texas Causes of Action for Unauthorized Disclosure of Private Health Information*

Individuals seeking relief for unauthorized disclosure of their medical records may pursue Texas statutory-based remedies and/or common law invasion of privacy causes of action. The following list is not exhaustive of all possible civil causes of action.

Individuals lack standing to sue for violations of HIPAA, the TMRPA, or the Texas Breach Notification Laws. However, the Texas Attorney General may pursue civil monetary penalties and injunctive relief for violations of these statutes.²⁵⁹

1. *Unauthorized Disclosure of Physician-Patient Communication:*

If a patient/person believes that he has been aggrieved by the unauthorized release of confidential communications and medical records, the person may file a

lawsuit against the person who disclosed the confidential information and seek injunctive relief and a cause of action for civil damages.²⁶⁰ The duty of confidentiality that arises under the statute results from the physician-patient relationship; the duty does not exist independent of the relationship.²⁶¹ Any duty a physician has to maintain the confidentiality of a health-care communication is inextricably intertwined with the physician-patient relationship and the health-care services to which the communication pertains.²⁶²

2. *Unauthorized Disclosure of Hospital Record:*

A patient may pursue injunctive relief and damages for the unauthorized release of his hospital patient records.²⁶³

3. *Unauthorized Disclosure of HIV-Related Test Results:*

A person who is injured by an issuer's violation of HIV-related test results may bring a civil action for damages. If the defendant released or allowed the test results to become known, the defendant could be found liable for actual damages or a civil penalty of not more than \$1000 if the release or disclosure was negligent, and between \$1000 to \$5000 if the release or disclosure was willful.²⁶⁴

It is a Class A misdemeanor to release or disclose an HIV-related test result or allow a test result or other information to become known.²⁶⁵ Each release or disclosure in violation of this code constitutes a separate offense.²⁶⁶

4. *Unauthorized Disclosure of Genetic Test:*

Disclosure of confidential genetic information carries a civil penalty not to exceed \$10,000.²⁶⁷

5. *Release of Re-Identified Records:*

The Attorney General for the State of Texas has the authority to institute an action for injunctive relief to restrain violators from releasing re-identified records under TEX. HEALTH & SAFETY CODE § 181.151 and impose civil money penalties.²⁶⁸ The civil penalty may not exceed \$3,000 for each violation, and if the court presiding over the injunctive relief action makes a finding that the violations occurred with a frequency as to constitute a pattern or practice, the court may assess a civil penalty not to exceed \$250,000.²⁶⁹

V. TEXAS STATE LAW PREEMPTION

Generally, if Texas privacy laws are contrary to HIPAA and HITECH, then HIPAA and HITECH will preempt Texas law.²⁷⁰ In this context, if a law is “contrary,” it means that it would be impossible for a covered entity to comply with both the Texas and federal requirements, or that Texas law stands as an obstacle to accomplishing the full purposes and objectives of HIPAA and HITECH.²⁷¹ There are exceptions to this general rule of federal preemption for contrary state laws. Under these exceptions, Texas privacy laws will apply if they:

- (1) Provide greater privacy protections or privacy rights with respect to PHI;
- (2) Provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention; or
- (3) Require certain health plan reporting, such as for management or financial audits.²⁷²

In addition, Texas privacy laws will apply if HHS determines, in response to a request from Texas or another entity or person, that the Texas law:

- (1) Is necessary to prevent fraud and abuse related to the provision of or payment for health care;
- (2) Is necessary to ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
- (3) Is necessary for Texas’ reporting on health care delivery or costs;
- (4) Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
- (5) Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by Texas law.²⁷³

VI. CONCLUSION

In November 2004, the Office of the Texas Attorney General published a report titled, “HIPAA Preemption Analysis Report” (TAG Report),²⁷⁴ which provides preemption analysis of Texas health care information privacy laws and HIPAA. According to the TAG Report, generally, most of the Texas laws reviewed were found not to be preempted by HIPAA because it is not impossible to comply with both laws, and Texas law does not appear to pose an obstacle to the purposes of HIPAA.²⁷⁵

However, the TAG Report noted there are many provisions in Texas law that may not rise to the level of the HHS definition of “contrary” but that may be in tension or conflict with HIPAA. For instance, Texas law does not contain provisions comparable to those in HIPAA such as “business associate contracts” and “organized health care arrangements.” Additionally, Texas law does not incorporate the broad disclosures authorized in HIPAA’s section for “treatment, payment, and health care operations.” Moreover, both HIPAA and Texas state law outline requisites for written authorization,²⁷⁶ but Texas law refers to such written authorizations in various statutes using different terms, such as “consent,” “consent form,” “release,” “written release,” or “written consent.”²⁷⁷ To further complicate this issue, HIPAA provides for permissive use of PHI with written *consent*, which is distinguished separate and apart from the requisite written *authorization*.²⁷⁸ For an authorization form to be consistent with both HIPAA and Texas laws, it needs to contain both HIPAA and Texas requisite core elements.

HIPAA and HITECH entail complex laws and regulations. HIPAA preemption analysis is an ongoing process as the healthcare legal community continues to comprehend and interpret these laws and regulations with the corresponding agency-issued guidance.

END NOTES

- ¹ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (1996) (HIPAA”), *codified in* 45 C.F.R. Parts 160 and 164.
- ² 45 C.F.R. Part 160 and Part 164, Subparts A and E.
- ³ American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, H.R. 1 (2009) (*enacted as the Health Information Technology for Economic and Clinical Health Act (HITECH) in Title XIII, Div. A, and Title IV, Div. B*).
- ⁴ TEX. OCC. CODE §§ 151.000-167.011.
- ⁵ TEX. HEALTH & SAF. CODE CHAP. 181.
- ⁶ American Medical Association, *Patient Confidentiality*, available through <http://www.ama-assn.org/ama/pub/physician-resources/legal-topics>.
- ⁷ American Medical Association Council on Ethical and Judicial Affairs, *Code of Medical Ethics* (2010-2011 ed.), available at <http://www.ama-assn.org>; TEX. OCC. CODE §§ 159.001, *et seq.*
- ⁸ *Patient Confidentiality*, *supra* note 6; *see also Code of Medical Ethics*, *supra* note 7.
- ⁹ *Id.*
- ¹⁰ *Id.*
- ¹¹ *See Whalen v. Roe*, 429 U.S. 589, 598-601 (1977); *Roe v. Wade*, 410 U.S.113, 153-154 (1973).
- ¹² *Whalen*, 429 U.S. at 598-601.
- ¹³ *Roe*, 410 U.S. at 154-155.
- ¹⁴ *Patient Confidentiality*, *supra* note 6.
- ¹⁵ *Id.*
- ¹⁶ HIPAA, *supra* note 1.
- ¹⁷ Department of Health and Human Services (HHS), *Summary of Privacy Rule, at 1*, available through <http://www.hhs.gov>; *see also* Report of the Office of the Attorney General of Texas, *Preemption Analysis of Texas Laws Relating to Privacy of Health Information and the Health Information Portability and Accountability Act and Privacy Rules (HIPAA)*, November 4, 2004, available at <http://www.oag.state.tx.us/notice/hipaa.pdf>.
- ¹⁸ *See* 65 Fed. Reg. 82,462, at 82,464 (2000).
- ¹⁹ For more discussion on PHI, *see infra* notes 39 through 44 and accompanying text.
- ²⁰ HHS, *The Privacy Rule*, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html>.
- ²¹ *Summary of Privacy Rule*, *supra* note 17, at 1.
- ²² *Id.*
- ²³ HHS, *The Security Rule*, available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/>.
- ²⁴ *See* HITECH, *supra*, note 3.
- ²⁵ HHS News Release, *HHS Strengthens Privacy and Security through New Rules*, July 8, 2010, available through <http://www.hhs.gov/news>. HITECH not only cites and cross-references various HIPAA definitions and privacy provisions, but it also expressly states the HIPAA privacy rules governing PHI shall remain in effect to the extent they are consistent with the new HITECH privacy rules. HHS is under a mandate to amend the HIPAA privacy rules, as necessary, to ensure consistency with HITECH. ARRA, *supra* note 3, at Title XIII, Subt. D, §13421(b).
- ²⁶ 45 C.F.R. §§ 160.102, 160.103.
- ²⁷ *Summary of Privacy Rule*, *supra* note 17, at 2.
- ²⁸ 45 C.F.R. §§ 160.102, 160.103; *see* Social Security Act § 1172(a)(3), 42 U.S.C. § 1320d-1(a)(3). The transaction standards are established by the HIPAA Transactions Rule at 45 C.F.R. Part 162.
- ²⁹ *Summary of Privacy Rule*, *supra* note 17, at 2-3.
- ³⁰ 45 C.F.R. § 160.103.
- ³¹ *Summary of Privacy Rule*, *supra* note 17, at 3.
- ³² 45 C.F.R. § 164.500(b).
- ³³ 45 C.F.R. §§ 160.103, 164.502(e), 164.504(e), 164.532(d) and (e); U.S. Department of Health and Human Services (HHS), Office of Civil Rights, *Guidance: Significant Aspects of the Privacy Rule:*

Business Associates,

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html>.

³⁴ *Id.*

³⁵ *Summary of Privacy Rule, supra* note 17, at 3.

³⁶ 45 C.F.R. §164.504(e); *see also Guidance, supra* note 34.

³⁷ 45 C.F.R. 164.504(e)(3).

³⁸ *Summary of Privacy Rule, supra* note 17, at 3.

³⁹ *Id.* at 3-4.

⁴⁰ 45 C.F.R. §160.103

⁴¹ 45 C.F.R. § 164.514(b)(2)(i).

⁴² Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (2008).

⁴³ *See* 74 Fed. Reg. 51,696, at 51,700 (2009).

⁴⁴ *See* HHS, *Health Information Privacy: Genetic Information, available at*

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/genetic/index.html>.

⁴⁵ 45 C.F.R. § 164.514(a); HHS, Office of Civil Rights, Workshop on HIPAA Privacy Rule’s De-identification Standard, *available through* <http://www.hhs.gov/ocr/privacy/hipaa/understanding>.

⁴⁶ 45 C.F.R. § 164.514(b).

⁴⁷ 45 C.F.R. § 164.514(b)(2). The following identifiers of the individual or of relatives, employers, or household members of the individual must be removed to achieve the “safe harbor” method of de-identification: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census (1) the geographic units formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000; (C) All elements of dates (except year) for dates directly related to the individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers; (N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met. In addition to the removal of the above-stated identifiers, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information.

⁴⁸ 45 C.F.R. § 164.514(b)(1).

⁴⁹ 45 C.F.R. §§ 164.502(d)(2), 164.514(a) and (b); *Summary of Privacy Rule, supra* note 17, at 4.

⁵⁰ 45 C.F.R. § 164.502(a).

⁵¹ 45 C.F.R. § 164.524.

⁵² 45 C.F.R. § 164.502(a)(2).

⁵³ 45 C.F.R. § 164.501.

⁵⁴ 45 C.F.R. § 164.512.

⁵⁵ 45 C.F.R. § 164.502(a)(1).

⁵⁶ 45 C.F.R. § 164.508(a)(2).

⁵⁷ 45 C.F.R. § 164.506(c).

⁵⁸ *Summary of Privacy Rule, supra* note 17, at 5.

⁵⁹ 45 C.F.R. § 164.501; *Summary of Privacy Rule, supra* note 17, at 5.

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² 45 C.F.R. § 164.506(b).

⁶³ *Summary of Privacy Rule, supra* note 17, at 5.

⁶⁴ *Id.* at 6.

⁶⁵ 45 C.F.R. § 164.510(a); *Summary of Privacy Rule, supra* note 17, at 6.

⁶⁶ 45 C.F.R. § 164.510(b).

⁶⁷ *Summary of Privacy Rule, supra* note 17, at 6.

⁶⁸ 45 C.F.R. §§ 164.502(a)(1)(iii); *Summary of Privacy Rule, supra* note 17, at 6.

⁶⁹ 45 C.F.R. § 164.512.

⁷⁰ *Summary of Privacy Rule, supra* note 17, at 7.

⁷¹ 45 C.F.R. § 164.512(a); *Summary of Privacy Rule, supra* note 17, at 7.

⁷² 45 C.F.R. § 164.512(b); *Summary of Privacy Rule, supra* note 17, at 7.

⁷³ 45 C.F.R. § 164.512(a), (c); *Summary of Privacy Rule, supra* note 17, at 7.

⁷⁴ 45 C.F.R. § 164.512(d); *Summary of Privacy Rule, supra* note 17, at 7.

⁷⁵ 45 C.F.R. § 164.512(e); *Summary of Privacy Rule, supra* note 17, at 7.

⁷⁶ 45 C.F.R. § 164.512(f); *Summary of Privacy Rule, supra* note 17, at 7.

⁷⁷ 45 C.F.R. § 164.512(g); *Summary of Privacy Rule, supra* note 17, at 7.

⁷⁸ 45 C.F.R. § 164.512(h); *Summary of Privacy Rule, supra* note 17, at 7.

⁷⁹ *Summary of Privacy Rule, supra* note 17, at 5. The Privacy Rule defines research as, “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” 45 C.F.R. § 164.501.

⁸⁰ 45 C.F.R. § 164.512(i); *Summary of Privacy Rule, supra* note 17, at 8.

⁸¹ 45 C.F.R. § 164.512(k); *Summary of Privacy Rule, supra* note 17, at 8.

⁸² 45 C.F.R. § 164.512(l); *Summary of Privacy Rule, supra* note 17, at 8.

⁸³ 45 C.F.R. § 164.514(e). A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; (xvi) Full face photographic images and any comparable images. *See* 45 C.F.R. § 164.514(e)(2).

⁸⁴ 45 C.F.R. § 164.508; *Summary of Privacy Rule, supra* note 17, at 9.

⁸⁵ A covered entity may condition the provision of health care solely to generate protected health information for disclosure to a third party on the individual giving authorization to disclose the information to the third party. For example, a covered entity physician may condition the provision of a physical examination to be paid for by a life insurance issuer on an individual’s authorization to disclose the results of that examination to the life insurance issuer. A health plan may condition enrollment or benefits eligibility on the individual giving authorization, requested before the individual’s enrollment, to obtain protected health information (other than psychotherapy notes) to determine the individual’s eligibility or enrollment or for underwriting or risk rating. A covered health care provider may condition treatment related to research (e.g., clinical trials) on the individual giving authorization to use or disclose the individual’s protected health information for the research.

⁸⁶ Examples of disclosures that would require an individual’s authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer of the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes; *see Summary of Privacy Rule, supra* note 17, at 8.

⁸⁷ 45 C.F.R. § 164.532; *Summary of Privacy Rule, supra* note 17, at 8.

⁸⁸ 45 C.F.R. § 164.508(a)(2).

⁸⁹ 45 C.F.R. § 164.508(a)(3)(i),(ii).

⁹⁰ *Summary of Privacy Rule, supra* note 17, at 8.

⁹¹ “Psychotherapy notes” mean notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the of the individual’s medical record. Psychotherapy notes excludes medication

prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R. § 164.501.

⁹² 45 C.F.R. § 164.508(a)(2)(i) and (ii).

⁹³ *Summary of Privacy Rule*, *supra* note 17, at 9.

⁹⁴ 45 C.F.R. § 164.501.

⁹⁵ 45 C.F.R. § 164.508(a)(3)(i)(A) or (B).

⁹⁶ *Summary of Privacy Rule*, *supra* note 17, at 9.

⁹⁷ 45 C.F.R. § 164.501

⁹⁸ 45 C.F.R. § 164.508(a)(3)(ii).

⁹⁹ 45 C.F.R. §§ 164.502(b), 164.514 (d); *Summary of Privacy Rule*, *supra* note 17, at 10.

¹⁰⁰ It is significant to note that, HITECH outlined a two-tiered-approach for analyzing “minimum necessary” PHI, but this approach was under a sunset provision and expired on August 17, 2010, pending the deadline when HHS was required to issue new guidance on the HIPAA “minimum necessary” standard. *See* HITECH, *supra*, note 3, at Title XIII, Subt. D, § 13405(b)(1)(B), (C). *See also* Cynthia S. Marietta, *Deadline Here to Comply with HITECH Act’s Restrictions on Uses, Disclosures, and Requests for Protected Health Information*, Feb. 2010, <http://www.law.uh.edu/healthlaw/perspectives/homepage.asp>.

¹⁰¹ 75 Fed. Reg. 40896.

¹⁰² *Summary of Privacy Rule*, *supra* note 17, at 10.

¹⁰³ *Summary of Privacy Rule*, *supra* note 17, at 5.

¹⁰⁴ 45 C.F.R. §§ 164.520(a) and (b). A group health plan, or a health insurer or HMO with respect to the group health plan, that intends to disclose protected health information (including enrollment data or summary health information) to the plan sponsor, must state that fact in the notice. Special statements are also required in the notice if a covered entity intends to contact individuals about health-related benefits or services, treatment alternatives, or appointment reminders, or for the covered entity’s own fundraising.

¹⁰⁵ 45 C.F.R. § 164.522(a)(1)(vi).

¹⁰⁶ 45 C.F.R. § 164.524.

¹⁰⁷ 45 C.F.R. § 164.501.

¹⁰⁸ A covered entity may deny an individual access, provided that the individual is given a right to have such denials reviewed by a licensed health care professional (who is designated by the covered entity and who did not participate in the original decision to deny), when a licensed health care professional has determined, in the exercise of professional judgment, that: (a) the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; (b) the protected health information makes reference to another person (unless such other person is a health care provider) and the access requested is reasonably likely to cause substantial harm to such other person; or (c) the request for access is made by the individual’s personal representative and the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person. A covered entity may deny access to individuals, without providing the individual an opportunity for review, in the following protected situations: (a) the protected health information falls under an exception to the right of access; (b) an inmate request for protected health information under certain circumstances; (c) information that a provider creates or obtains in the course of research that includes treatment for which the individual has agreed not to have access as part of consenting to participate in the research (as long as access to the information is restored upon completion of the research); (d) for records subject to the Privacy Act, information to which access may be denied under the Privacy Act, 5 U.S.C. § 552a; and (e) information obtained under a promise of confidentiality from a source other than a health care provider, if granting access would likely reveal the source. 45 C.F.R. § 164.524; *Summary of Privacy Rule*, *supra* note 17, at 12-13.

¹⁰⁹ *Summary of Privacy Rule*, *supra* note 17, at 12-13.

¹¹⁰ 45 C.F.R. § 164.526.

¹¹¹ Covered entities may deny an individual’s request for amendment only under specified circumstances. A covered entity may deny the request if it: (a) may exclude the information from access by the individual; (b) did not create the information (unless the individual provides a

reasonable basis to believe the originator is no longer available); (c) determines that the information is accurate and complete; or (d) does not hold the information in its designated record set. 164.526(a)(2).

¹¹² *Summary of Privacy Rule, supra* note 17, at 12-13.

¹¹³ 45 C.F.R. § 164.528(a); *see id.* at 13.

¹¹⁴ 45 C.F.R. § 164.528(a)(1)(iv). A covered entity's compliance date is the date by which it was required to comply with the standards, implementation specifications, requirements, or modifications adopted by the HIPAA Administrative Standards, as defined in 45 C.F.R. § 160.103; *see also Summary of Privacy Rule, supra* note 17, at 13.

¹¹⁵ 45 C.F.R. § 164.528 (a).

¹¹⁶ *Id.*

¹¹⁷ Electronic health record (EHR) is defined in HITECH to mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. *See* HITECH *supra* note 3, at Tit. XIII, Subt. D, § 13400(5).

¹¹⁸ 45 C.F.R. § 164.522(a).

¹¹⁹ *Id.* at (1)(vi).

¹²⁰ *Id.* at (1)(iii). In addition, a restriction agreed to by a covered entity is not effective under this subpart to prevent uses or disclosures permitted or required under §§ 164.502(a)(2)(ii), 164.510(a) or 164.512; *Summary of Privacy Rule, supra* note 17, at 13.

¹²¹ 45 C.F.R. § 164.502(g)(1-4).

¹²² 45 C.F.R. § 164.502(g).

¹²³ *See* for example and without limitation, TEX. OCC. CODE § 151.002(6); TEX. HEALTH & SAF. CODE § 166.164; and TEX. PROB. CODE § 3, which provides that the following are legally authorized representatives in various circumstances:

- (1) a parent or legal guardian if the patient is a minor;
- (2) a legal guardian if the patient has been adjudicated incompetent to manage the patient's personal affairs;
- (3) an agent of the patient authorized under a durable power of attorney for health care;
- (4) an attorney ad litem appointed for the patient;
- (5) a guardian ad litem appointed for the patient;
- (6) a personal representative or statutory beneficiary if the patient is deceased;
- (7) an attorney retained by the patient or by another person listed herein; or
- (8) If an individual is deceased, their personal representative must be the executor, independent executor, administrator, independent administrator, or temporary administrator of the estate.

¹²⁴ *Summary of Privacy Rule, supra* note 17, at 16.

¹²⁵ *Id.*

¹²⁶ *Id.* at 17.

¹²⁷ *See* HITECH, *supra* note 3, at Tit. XIII, Subt. D, § 13410.

¹²⁸ *Id.*

¹²⁹ HHS News Release, *HHS Strengthens Privacy and Security through New Rules*, July 8, 2010, available through <http://www.hhs.gov/news>. HITECH not only cites and cross-references various HIPAA definitions and privacy provisions, but it also expressly states the HIPAA privacy rules governing PHI shall remain in effect to the extent they are consistent with the new HITECH privacy rules. HHS is under a mandate to amend the HIPAA privacy rules, as necessary, to ensure consistency with HITECH. HITECH, *supra* note 3, at Title XIII, Subt. D, § 13421(b).

¹³⁰ *See* HITECH *supra* note 3, at § 13424; *see also Modifications to HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act (Modifications NPRM)*, 75 Fed. Reg. 40867 (proposed July 14, 2010).

¹³¹ *Id.* at § 13405(e); *see also Modifications to HIPAA Privacy, Security, and Enforcement Rules* 75 Fed. Reg. at 40868.

¹³² *See* HITECH *supra* note 3, at § 13405(a).

¹³³ *See* definition of "business associate," *supra* notes 34 – 36 and accompanying text.

¹³⁴ *See* HITECH *supra* note 3, at §§ 13401(a), (b); 13408. *See* definition of "business associate agreement," *supra* notes 36 – 38 and accompanying text.

¹³⁵ *Id.* at § 13408.

¹³⁶ *Id.* at §§ 13402; 13407.

¹³⁷ *Id.* at §§ 13402.

¹³⁸ 74 Fed. Reg. 42740 (August 24, 2009).

¹³⁹ 74 Fed. Reg. 42962 (August 25, 2009).

¹⁴⁰ The HIPAA Breach Final Rule (Regulation Identifier Number (RIN) 0991-AB56) had been at the Office of Management and Budget (OMB) since May 14, 2010, for Executive Order (EO) 12866 review and approval prior to publication in the *Federal Register*. On July 28, 2010, HHS “withdrew” this Final Rule, with the following explanation: “HHS reviewed the public comment on the interim rule and developed a final rule, which was submitted to the Office of Management and Budget (OMB) for Executive Order 12866 regulatory review on May 14, 2010. At this time, however, HHS is withdrawing the breach notification final rule from OMB review to allow for further consideration, given the Department’s experience to date in administering the regulations. This is a complex issue and the Administration is committed to ensuring that individuals’ health information is secured to the extent possible to avoid unauthorized uses and disclosures, and that individuals are appropriately notified when incidents do occur. We intend to publish a final rule in the Federal Register in the coming months. Until such time as a new final rule is issued, the Interim Final Rule that became effective on September 23, 2009, remains in effect.” On February 9, 2011, HHS submitted revisions for OMB review, which are still pending, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html>.

¹⁴¹ Electronic health record (EHR) is defined in HITECH to mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. *See* HITECH *supra* note 3, at Tit. XIII, Subt. D, §13400(5).

¹⁴² *See* HITECH *supra* note 3, at § 13405(c).

¹⁴³ 75 Fed. Reg. 23214, 23215-16 (2010).

¹⁴⁴ *Id.* at 23215-16.

¹⁴⁵ HITECH *supra* note 3, at § 13406.

¹⁴⁶ HITECH *supra* note 3, at § 13405(d).

¹⁴⁷ 45 C.F.R. § 164.501.

¹⁴⁸ *See* HITECH, *supra* note 3, at § 13410.

¹⁴⁹ *See* HITECH, *supra* note 3, at § 13410(a)-(d).

¹⁵⁰ *See* HITECH, *supra* note 3, at § 13410(e).

¹⁵¹ *See* HITECH, *supra* note 3, at § 13411.

¹⁵² *See* HITECH, *supra* note 3, at § 13409.

¹⁵³ Consumer Partnership for eHealth, *Protecting Sensitive Health Information in the Context of Health Information Technology*, June 2010, available through <http://www.nationalpartnership.org>. The HIPAA Privacy Rule does not draw a distinction between SHI or other health information. The National Committee on Vital and Health Statistics, which is HHS’ public advisory body on health data, statistics and national information policy, has recognized certain defined categories of sensitive information. *See generally* National Committee on Vital and Health Statistics, *Correspondence to Kathleen Sebelius*, Nov. 10, 2010.

¹⁵⁴ *Correspondence to Kathleen Sebelius*, *supra* note 153, at 1.

¹⁵⁵ *Protecting Sensitive Health Information*, *supra* note 153, at 2-3; *see also* *Correspondence to Kathleen Sebelius*, *supra* note 153, at 4-13.

¹⁵⁶ TEX. OCC. CODE § 159.001, *et seq.*

¹⁵⁷ TEX. OCC. CODE § 159.002(a); *see M utter v. Wood*, 744 S.W.2d 600, 600-01 (Tex. 1988); *Hogue v. Kroger Store*, 875 S.W.2d 477, 480 (Tex. App. -- Houston [1st Dist.] 1994, writ denied).

¹⁵⁸ TEX. OCC. CODE § 159.002(b); *see, e.g., Sloan v. Farmer*, 217 S.W.3d 763, 768 (Tex. App. -- Dallas 2007, pet. denied).

¹⁵⁹ WEBSTER’S NINTH NEW COLLEGIATE DICTIONARY 275 (1985).

¹⁶⁰ *Id.* at 936.

¹⁶¹ *Id.* at 768.

¹⁶² *Id.*

¹⁶³ *Id.*

¹⁶⁴ TEX. OCC. CODE § 159.002.

¹⁶⁵ TEX. OCC. CODE § 159.002(a), (b).
¹⁶⁶ TEX. OCC. CODE § 159.002(e).
¹⁶⁷ *Id.*
¹⁶⁸ *See* TEX. OCC. CODE § 159.002(d).
¹⁶⁹ TEX. OCC. CODE § 159.003.
¹⁷⁰ TEX. OCC. CODE § 159.004.
¹⁷¹ *Id.*
¹⁷² *See R.K. v. Ramirez*, 887 S.W.2d 836, 840 (Tex. 1994).
¹⁷³ *Id.* at 840.
¹⁷⁴ *Id.*
¹⁷⁵ TEX. OCC. CODE § 159.005(a).
¹⁷⁶ TEX. OCC. CODE § 159.005(a)-(b).
¹⁷⁷ TEX. OCC. CODE § 159.005(c).
¹⁷⁸ TEX. OCC. CODE § 159.005(e).
¹⁷⁹ *See* TEX. OCC. CODE § 159.002(c), 159.005(e); *In re Xeller*, 6 S.W.3d 618, 625 (Tex. App. -- Houston [14th Dist.] 1999, orig. proceeding) (finding that just because a claimant filed a medical claim with his insurance company does not mean he consented to the insurance company making his medical records public).
¹⁸⁰ *In re Tenet Healthcare Ltd.*, No. 12-05-00310-CV, 2006 WL 860076, at *2 (Tex. App. -- Tyler, March 31, 2006, orig. proceeding); *In re Columbia Valley Regional Med. Ctr.*, 41 S.W.3d 797, 802 (Tex. App. -- Corpus Christi 2001, orig. proceeding).
¹⁸¹ *In re Columbia Valley Regional Med. Ctr.*, 41 S.W.3d at 800 (concluding confidentiality is not limited to identity of the patient, only).
¹⁸² *See id.* at 803 (finding the privacy rights of the patients would be violated if the redacted medical records were disclosed without the patient's consent); *see also Xeller*, 6 S.W.3d at 625.
¹⁸³ TEX. HEALTH & SAFETY CODE § 181.151.
¹⁸⁴ *See In re Columbia Valley Regional Medical Ctr.*, 41 S.W.3d at 802; *In re Xeller*, 6 S.W.3d at 625; *Tarrant Cty. Hosp. Dist. v. Hughes*, 734 S.W.2d 675, 678 (Tex. App. -- Fort Worth 1987, orig. proceeding) (citing *Whalen v. Roe*, 429 U.S. 589, 598-601 (1977)); *see also* Op. Tex. Att'y Gen. ORD-370 (1983).
¹⁸⁵ *Whalen*, 429 U.S. at 598-601.
¹⁸⁶ TEX. OCC. CODE §§ 201.402, 201.405 (chiropractors); TEX. OCC. CODE §§ 202.406 (podiatrists); TEX. OCC. CODE §§ 258.102, 258.104 (dentists).
¹⁸⁷ TEX. HEALTH & SAF. CODE § 181.001(b)(2).
¹⁸⁸ *Id.*
¹⁸⁹ *Id.* at § 181.151.
¹⁹⁰ TEX. HEALTH & SAF. CODE § 241.153.
¹⁹¹ TEX. HEALTH & SAF. CODE Chap. 242; 40 TEX. ADMIN. CODE §§ 19.407, 19.413.
¹⁹² TEX. HEALTH & SAF. CODE Chap. 252; 40 TEX. ADMIN. CODE Chap. 19.
¹⁹³ TEX. HEALTH & SAF. CODE Chap. 243.
¹⁹⁴ TEX. HEALTH & SAF. CODE Chap. 254.
¹⁹⁵ *Id.*
¹⁹⁶ TEX. HEALTH & SAF. CODE §§ 611.001 – 611.008.
¹⁹⁷ *Id.* at §§ 611.002 – 611.004.
¹⁹⁸ TEX. HEALTH & SAF. CODE §§ 611.002.
¹⁹⁹ *See id.*
²⁰⁰ TEX. HEALTH & SAF. CODE §§ 611.004.
²⁰¹ *See e.g.*, TEX. HEALTH & SAF. CODE §§ 572.004, 576.007, 595.005.
²⁰² 20 U.S.C. § 1232g; 34 C.F.R. Part 99.
²⁰³ *See infra* notes 240-247 and accompanying text.
²⁰⁴ TEX. HEALTH & SAF. CODE § 81.103(a); TEX. INS. CODE § 545.057
²⁰⁵ TEX. HEALTH & SAF. CODE § 81.103(a); TEX. INS. CODE § 545.057.
²⁰⁶ TEX. HEALTH & SAF. CODE §§ 81.103(j); 81.104.
²⁰⁷ TEX. HEALTH & SAF. CODE § 85.260.
²⁰⁸ TEX. GOV'T CODE § 501.054.
²⁰⁹ TEX. HEALTH & SAF. CODE § 85.115.

210 TEX. HEALTH & SAF. CODE § 81.046 .

211 *Id.*

212 *Id.*

213 TEX. HEALTH & SAF. CODE §§ 81.047, 81.052.

214 TEX. HEALTH & SAF. CODE § 81.046.

215 Pub. L. 110-223, 122 Stat. 881 (2008).

216 TEX. OCC. CODE § 58.102, 58.104.

217 TEX. OCC. CODE § 58.103.

218 TEX. HEALTH & SAF. CODE Chap. 611 AND § 464.009.

219 25 TEX. ADMIN. CODE §§ 444.303, 448.210.

220 42 U.S.C. §290dd-2 (2006); 42 C.F.R. Part 2.

221 *Correspondence to Kathleen Sebelius, supra* note 153, at 7.

222 42 U.S.C. § 290dd-2(a) and (e); *see also* TEX. HEALTH & SAF. CODE Chap. 611, Chap. 159.

223 TEX. HEALTH & SAF. CODE § 161.021.

224 TEX. HEALTH & SAF. CODE § 161.022.

225 TEX. HEALTH & SAF. CODE § 161.0213.

226 TEX. HEALTH & SAF. CODE § 84.004.

227 TEX. HEALTH & SAF. CODE § 84.006.

228 *Id.*

229 *See, e.g.,* TEX. FAMILY CODE Chap. 32; TEX. HUMAN RESOURCES CODE Chap. 48; TEX. HEALTH & SAF. CODE Chap. 614; TEX. PROB. CODE Chap. XII.

230 TEX. HEALTH & SAF. CODE § 241.1531.

231 20 U.S.C. §1232g; 34 C.F.R. Part 99.

232 34 C.F.R. § 99.31.

233 TEX. HEALTH & SAF. CODE §595.005(c).

234 TEX. GOV'T CODE §560.001.

235 TEX. GOV'T CODE §560.002.

236 *Id.*

237 TEX. GOV'T CODE §560.003.

238 42 U.S.C. §1396a(a)(7); 42 C.F.R. §431.300(a); 42 C.F.R. § 431.305; 42 C.F.R. § 431.302; 42 C.F.R. §431.306(d); 42 C.F.R. §457.1110; TEX. HUMAN RESOURCES CODE §§12.003, 21.012; and TEX. GOV'T CODE §533.009.

239 42 U.S.C. § 1771, *et seq.*

240 42 U.S.C. § 1751, *et seq.*

241 42 U.S.C. § 1758 (b).

242 Title XXI of the Social Security Act, 42 U.S.C. Chap. 7, Subchap. XXI, §1397aa-1397mm.

243 *See* §1902(a)(7) of the Social Security Act; 42 U.S.C. §1396a (a)(7); 42 C.F.R. §431.301; 42 C.F.R. §457.1110; *see also* TEX. HEALTH & SAFETY CODE Chap. 62, Subchap. B, Chap. 63; 1 TEX. ADMIN. CODE Part 15, Subchap. 370.

244 The federal regulations for protection and advocacy systems are found in 42 C.F.R. Part 51. Texas established Advocacy, Inc. as the protection and advocacy authority in Texas. *See* TEX. Human Resources Code §112.021; TEX. HEALTH & SAFETY CODE §576.008, 1 TEX. ADMIN. CODE §414.5; *see also* TEX. HEALTH & SAFETY CODE §615.002; 40 TEX. ADMIN. CODE §19.1413.

245 DD Act, 42 U.S.C. §§ 15001-115 (2006).

246 PAIMI Act, 42 U.S.C. § 10801-851 (2006).

247 PAIR Act, 29 U.S.C. § 794e (2006).

248 42 U.S.C. § 15043(a)(2)(B); 42 U.S.C. § 10805(a)(1)(A); 29 U.S.C. § 794e(f)(2); 45 C.F.R. § 1386.19; 42 C.F.R. § 51.2.

249 42 U.S.C. § 15043(a)(2)(A)(i); 42 U.S.C. § 10805(a)(1); 29 U.S.C. § 794e(f)(3).

250 42 U.S.C. § 15043(a)(2)(H)-(I); 42 U.S.C. § 10805(a); 29 U.S.C. § 794e(f)(2).

251 42 U.S.C. § 15043(a)(2)(I)(i); 42 U.S.C. § 10805(a)(4)(A); 29 U.S.C. § 794e(f)(2).

252 TEX. BUS. & COM. CODE Chap. 521.

253 *Id.*

254 *Id.*

255 TEX. GOV'T CODE Chap. 552.

²⁵⁶ TEX. OCC. CODE § 151.002(a)(8); TEX. HEALTH & SAF. CODE §§ 161.0315, 161.032.

²⁵⁷ TEX. OCC. CODE §§ 160.006(c),(d); 160.007.

²⁵⁸ TEX. OCC. CODE § 160.007; TEX. HEALTH & SAF. CODE § 161.032.

²⁵⁹ See HITECH, *supra* note 3, at § 13410(e); TEX. HEALTH & SAF. CODE § 181.201; TEX. BUS. & COM. CODE § 521.151.

²⁶⁰ TEX. OCC. CODE § 159.009(a), (b); *see also In re Xeller*, 6 S.W.3d at 618 (acknowledging violators may be subject to civil liability for the unauthorized disclosure of confidential medical records).

²⁶¹ *Sloan*, 217 S.W.3d at 768 (pursuing claim for violation of physician-patient confidentiality under the Texas Medical Records Privacy Act, among other claims).

²⁶² *Id.*

²⁶³ TEX. HEALTH & SAF. CODE § 241.152; *see also Foster ex rel. J.L. v. Hillcrest Baptist Med. Ctr.*, No. CV-10-02-143, 2004 WL 254713, at *5 (Tex. App. – Waco, Feb. 11, 2004, denied) (affirming plaintiff’s claim for violation of statute, TEX. HEALTH & SAF. CODE § 241.152, and common law cause of action for invasion of privacy).

²⁶⁴ TEX. INS. CODE § 545.703.

²⁶⁵ *Id.*; TEX. HEALTH & SAF. CODE §§ 81.103, 85.260.

²⁶⁶ TEX. INS. CODE § 545.703.

²⁶⁷ TEX. OCC. CODE § 58.105.

²⁶⁸ See TEX. HEALTH & SAF. CODE § 181.201(a), (b).

²⁶⁹ TEX. HEALTH & SAF. CODE § 181.201(c).

²⁷⁰ 45 C.F.R. § 160.203.

²⁷¹ 45 C.F.R. § 160.202; *Summary of Privacy Rule*, *supra* note 17, at 17.

²⁷² 45 C.F.R. § 160.202.

²⁷³ 45 C.F.R. § 160.203.

²⁷⁴ Report of the Office of the Attorney General of Texas, *supra* note 17, at 5 – 20.

²⁷⁵ *Id.* An updated version of his particular report has not been published since the enactment of HITECH. Additional updates may be required after issuance of the anticipated changes to HITECH breach notification requirements.

²⁷⁶ See 45 C.F.R. § 164.508(c)(1) (HIPAA authorization core elements) and TEX. CIV. PRAC. & REM. CODE § 74.052 (Texas Authorization form).

²⁷⁷ See, e.g., TEX. HEALTH & SAF. CODE §§ 81.103; 161.0073; 611.004; 611.006; TEX. OCC. CODE § 159.005.

²⁷⁸ See, e.g., HHS, *Health Information Policy: What is the Difference Between “Consent” and “Authorization” Under the HIPAA Privacy Rule?*, March 14, 2006, available at <http://www.hhs.gov/ocr/privacy/hipaa/faq/authorizations/264.html>.