



DAVISBROWN[®]

LAW FIRM



IMPORTANT HIPAA CHANGES

SUSAN J. FREED

THE DAVIS BROWN TOWER
215 10TH STREET, SUITE 1300
DES MOINES, IA 50309
515-288-2500
WWW.DAVISBROWNLAW.COM

DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

IMPORTANT HIPAA CHANGES

The American Recovery & Reinvestment Act of 2009 makes significant changes to the privacy and security regulations adopted under the Health Insurance Portability & Accountability Act ("HIPAA"). Some of the most significant changes include:

- making business associates directly subject to HIPAA's privacy and security requirements and applying criminal and civil monetary penalties to business associates who fail to comply;
- requiring covered entities to report security breaches to both the federal government and the individual whose information was breached; and
- mandating that civil monetary penalties be imposed against covered entities and business associates who violate HIPAA's privacy and security provisions.

Below is a summary of these and other HIPAA changes included in the American Recovery & Reinvestment Act. If you have any questions, please contact Susan Freed or your Davis Brown attorney.

1. Business Associates

"Business associates" are individuals or entities that provide services for a covered entity that require the use of protected health information. Examples include accountants, billing companies, collection agencies, information technology providers and attorneys. Business associates have not previously been directly subject to HIPAA's privacy and security provisions. Rather, they were required to comply with HIPAA only through contracts, referred to as "Business Associate Agreements" that were entered into between the covered entity and business associate. Because they were not subject to HIPAA, they could not be penalized by the federal government for failing to comply with HIPAA's provisions. The only penalties a business associate faced for failing to comply with HIPAA's provisions were the penalties provided for in the Business Associate Agreement.

The new law now applies HIPAA's privacy provisions to business associates. Business associates are also required to comply with HIPAA's security provisions relating to administrative, physical and technical safeguards. Business associates face criminal and civil monetary penalties for failing to comply with HIPAA.

The application of HIPAA directly to business associates appears to take effect on February 17, 2010, one year from enactment.

2. Required Notifications

Currently, HIPAA does not require covered entities to notify the federal government of a security breach which results in the unauthorized disclosure of protected health information. In addition, covered entities are not currently required to notify individuals that their health information has been compromised or disclosed in violation of the law unless such notification could mitigate the harm to the individual of the unauthorized use/disclosure.

When a Notice is Required. The Act now requires covered entities to notify an individual if the individual's "unsecured protected health information" has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of a breach. "Unsecured protected health information" is defined as protected health information that is not secured through the use of a technology or methodology specified by regulation as rendering the information unusable, unreadable, or indecipherable (i.e., information that is not encrypted).

For example, if an unauthorized individual hacks into a provider's computer system and downloads data that can later be retrieved and read, a reportable breach has occurred. However, if the provider has installed a technology or methodology approved by the regulations as protecting the information from being deciphered or read, the breach is not reportable.

Business associates who experience a breach of unsecured protected health information must notify the covered entity. The covered entity then has the responsibility of notifying the individual.

Timing of Notices. Notices to individuals must be provided without unreasonably delay and no later than 60 days after the discovery of the breach. A notice may be postponed only if a law enforcement official determines that the required notice would impede a criminal investigation or cause damage to national security.

Method of Providing Notices. The notice must be provided by first-class mail, unless the individual has requested communications through electronic mail. If the individual's current address is unknown, the covered entity may use a substitute form, including posting the information on its website or through the media. If the breach impacts more than 500 individuals of a particular State or jurisdiction, prominent media outlets serving the area must be notified.

Notice to Federal Government. Covered entities must also notify the Secretary of Health and Human Services ("HHS") of any unsecured protected health information that has been acquired or disclosed in a breach. The notice must be provided annually with respect to any breaches that occur during the

preceding year. If the breach was with respect to 500 or more individuals than notice must be provided immediately to the Secretary.

Content of Notices. All notices required by the new law must contain the following:

- a brief description of what happened, including the date of the breach and the date it was discovered;
- a description of the types of unsecured protected health information that were involved in the breach;
- the steps individuals should take to protect themselves from harm;
- a brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses and to protect against further breaches; and
- contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an email address, Web-site or postal address.

Effective Date. The required notice provisions apply to breaches that occur 30 days after the Secretary releases interim final regulations implementing these new notice requirements. The Secretary must release these regulations by August 16, 2009.

3. Vendors of Personal Health Records

The new law provides temporary provisions requiring vendors of personal health records to comply with the same security breach notification processes that covered entities must comply with, *provided, however*, the vendor must notify the FTC instead of HHS. Third party service providers of these covered vendors are required to notify the vendor of a breach in the same manner a business associate is required to notify a covered entity. Failure to comply with the law's requirements constitutes an unfair and deceptive trade practice enforceable by the FTC.

The law's provisions are "temporary" as they sunset if Congress enacts new legislation establishing requirements for individuals and entities not otherwise considered covered entities or business associates subject to HIPAA.

A "personal health record" is an electronic record of PHR identifiable information (i.e., PHI in the hands of a PHR vendor or third party service provider) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

4. Restrictions Requested by Individuals

Under the current law, an individual may request that a covered entity not release certain protected health information to a specific individual or entity; however, the covered entity does not have to comply unless the disclosure requires the individual's authorization.

Under the new law, an individual that has paid the full charge for an item or service out of pocket may request that a covered entity not disclose information relating to the item or service to a health plan. The covered entity **MUST** comply with the request. For example, a patient can require that a provider not release information relating to the patient's HIV test to a health plan if the patient pays for the HIV test in full.

5. Accounting of Disclosures of Electronic Health Records

Currently, individuals can request an accounting from a covered entity describing how their protected health information has been disclosed over the past 6 years, with the exception of disclosures for treatment, payment and health care operations ("TPO").

The new law expands the accounting requirement for covered entities that utilize electronic health records ("EHRs") by eliminating the exception for disclosures due to treatment, payment and health care operations and requiring that these disclosures be accounted for. However, the law applies only a 3 year accounting requirement for TPO disclosures instead of the 6 year requirement that applies to non-TPO disclosures.

For disclosures made by business associates utilizing EHRs, the covered entity may provide the accounting or may simply list the names and contact information for the business associates and require the business associates to provide the information to the requestor directly.

The effective date for the new accounting provisions is January 14, 2014 for EHRs acquired as of January 1, 2009. For EHRs acquired after January 1, 2009, the provision is effective on the later of January 1, 2011 or the date upon which the entity acquires the EHR. HHS can impose a later effective date but it can be no later than 2016 for EHRs acquired as of January 1, 2009 or 2013 for all other EHRs.

6. Individual Requests for Electronic Information

If an individual requests information from a covered entity that has an EHR, the covered entity must provide the individual with a copy of the information in electronic format, must transmit a copy directly to a recipient designated by an

individual and can only charge the fee associated with the covered entity's "labor costs."

7. Restrictions on Selling Information

Covered entities and business associates are prohibited from receiving remuneration (whether direct or indirect) in exchange for protected health information except pursuant to an individual's valid HIPAA authorization. There are numerous exceptions to this provision including exceptions for public health activities, research and treatment uses, transfers due to the sale of a business, or providing individuals with a copy of their protected health information.

This prohibition is effective for disclosures of protected health information that occur 180 days after HHS issues implementing regulations.

8. Marketing Communications

Prior to the new law, a covered entity could provide marketing communications without an individual's authorization if the communication was describing a health care item or service for treatment, case management or counseling purposes. These communications were considered health care operations.

The new law no longer provides for protection of these types of communications if the covered entity or business associate making the communication receives remuneration (direct or indirect) for making the communication. There are some exceptions for communications regarding medications currently being used by the individual and communications pursuant to an individual's authorization.

9. Fundraising

Prior versions of the bill would have limited covered entities' ability to utilize protected health information for fundraising purposes. The new law retains the current fundraising provisions; however, requires that covered entities provide individuals with the right to opt-out of further fundraising communications in a "clear and conspicuous manner."

10. Enforcement

The new law provides for what it refers to as "improved enforcement." The law amends HIPAA's enforcement provisions to require HHS to impose civil monetary penalties against individuals or entities that violate HIPAA. The only exception is where it is determined that the violator did not know and could not have known by exercising reasonable diligence that a violation of the law occurred. In addition, the new law requires HHS to formally investigate any

complaint that after a preliminary investigation indicates a possible violation due to willful neglect.

The law also requires the GAO to develop recommendations for providing individuals whose protected health information is the subject of a HIPAA violation with a portion of any civil monetary penalties collected from the covered entity or business associate as a result of the violation.

Finally, the new law allows State Attorney Generals to bring a civil action in federal district court against individuals who violate the HIPAA privacy and security provisions and to seek an injunction or civil monetary penalties against the individual. The State may also recover its attorneys' fees.

These enforcement provisions are effective for violations that occur after February 17, 2009, with the exception of the provisions relating to willful neglect violations which are effective on February 17, 2011.

If you have any questions regarding any of the new HIPAA provisions, please contact Susan Freed at (515) 246-7891 or via email at susanfreed@davisbrownlaw.com

Notice: Davis Brown updates are intended to provide general information about significant legal issues and should not be construed as legal advice regarding any specific facts or circumstances. You are encouraged to consult with appropriate legal counsel to address specific legal questions. This update is provided for informational purposes only as a service to clients of Davis Brown. This update is not intended and should not be construed as an advertisement for legal services

ATTORNEY BIO

SUSAN J. FREED

CONCENTRATION

Susan is a shareholder at the Davis Brown Law Firm where she has a general practice in, but not limited to, the areas of Health Law and Employee Benefits.

SUMMARY

Susan represents a wide variety of health care providers, including county hospitals and facilities, with respect to transactional, reimbursement, and regulatory issues. She drafts contracts, employment agreements, physician recruitment agreements, corporate documents and corporate policies. In addition, she counsels clients on various health law issues including fraud and abuse, Medicare and Medicaid reimbursement, EMTALA, medical staff relations, and confidentiality laws.

She also advises employers on employee welfare benefit issues including ERISA, COBRA and HIPAA, and assists individuals in appealing health and disability benefit denials. She has assisted several employer-sponsored health plans with their HIPAA privacy compliance efforts, including a large self-funded multiple employer welfare benefit plan. She has also successfully appealed insurance company denials of health benefits, including those based on a lack of medical necessity.

Susan counsels employers on affirmative action requirements and drafts affirmative action plans for employers.

MEMBERSHIPS

She is a current member of the Broadlawns Medical Center Foundation's Board of Directors. Susan is a graduate of the Greater Des Moines Leadership Institute (2002-2003).

PUBLICATIONS, SPEECHES, AND SEMINARS

Susan is a frequent presenter on health law and employee benefit issues including, wellness programs, the Iowa Smoke Free Air Act, and employee benefit issues.

She has co-authored the Employee Benefits Section of the Iowa Bar Association's Business Law Manual and wrote the Employee Benefit Section for the Iowa Human Resources Manual for the Iowa Association of Business and Industry. She taught a Health Law course at the Drake University Law School for four years.

ACADEMICS

Susan earned her law degree with a certificate in health law from DePaul University College of Law in Chicago, Illinois.



BORN
PAULINA, IOWA, 1973

EDUCATION
UNIVERSITY OF IOWA (B.S., 1996);
DEPAUL UNIVERSITY (J.D., 1999)

ADMITTED TO BAR
1999, IOWA
2000, ILLINOIS

AREAS OF LAW

- BUSINESS ORGANIZATIONS AND TRANSACTIONS
- EMPLOYEE BENEFITS
- HEALTH LAW
- REAL ESTATE

MEMBERSHIPS

- AMERICAN BAR ASSOCIATION
- AMERICAN HEALTH LAWYERS ASSOCIATION
- IOWA STATE BAR ASSOCIATION
- POLK COUNTY BAR ASSOCIATION

PRACTICE AREA

HEALTH LAW

The Davis Brown Law Firm represents clients in matters of general health care and hospital law, as well as in all matters connected with the operation and development of health care organizations, including litigation. Issues specific to health care organizations include legislative and regulatory issues, patient/resident issues, staff issues, certificates of need, third party payments, alternative health care delivery systems, licensing and accreditation, institutional review, policy and procedure development and implementation, physician contracts and compensation, and Medicare and Medicaid compliance.

The Firm also counsels clients on matters of medical ethics, such as withholding or withdrawing medical treatment. The Firm advises health care clients on a range of organizational issues incidental to health care delivery, including labor and employment law, compensation and benefits, mergers and acquisitions, joint ventures, antitrust, intellectual property, financing and taxation.

Davis, Brown, Koehn, Shors & Roberts, P.C. is general counsel to the Iowa Health Care Association, the state-wide association of long-term care facilities. The Firm represents a major medical center, regional and county hospitals, home health care agencies, life care facilities, nursing homes, physicians and other health care organizations.



ATTORNEYS WORKING IN THIS AREA

BOES, JUDITH "LYNN" R.

FREED, SUSAN J.

HOLZ, ROBERT F.

SHORS, JOHN D.

WATKINS, KENDALL R.

WHITNEY, JO ELLEN