Healthcare Practice

HIPAA/HITECH Act vs. Idaho's Data Breach Notification Statute

January 2010

GARVEY SCHUBERT BARER

Attorneys

BEIJING NEW YORK PORTLAND SEATTLE WASHINGTON, D.C.

HEALTHCARE PRACTICE

STEPHEN ROSE
SROSE@GSBLAW.COM
206.464.3939 EXT 1375

NANCY COOPER
NCOOPER@GSBLAW.COM

CARLA DEWBERRY
CDEWBERRY@GSBLAW.COM

DAVID GEE
DGEE@GSBLAW.COM

ROGER HILLMAN
RHILLMAN@GSBLAW.COM

ERIC LINDENAUER
ELINDENAUER@GSBLAW.COM

LAM NGUYEN-BULL
HQNGUYEN@GSBLAW.COM

EMILY STUDEBAKER
ESTUDEBAKER@GSBLAW.COM

SCOTT WARNER
SWARNER@GSBLAW.COM

HIPAA/HITECH Background

In 2003, the Health Information Portability and Accountability Act ("HIPAA") became effective. The purpose of HIPAA was to provide baseline federal protections for personal health information held by healthcare providers (termed "covered entities") and give patients an array of rights with respect to that information.

- In 2009, HIPAA was supplemented and enhanced by the Health Information Technology for Economic and Clinical Health Act ("HITECH"). HITECH imposes stricter enforcement penalties and details notification requirements to patients should their health information be improperly disclosed. In short, HIPAA/HITECH affects a very wide range of healthcare providers from hospitals, doctors, chiropractors, nursing homes to pharmacies and health plan providers -- as well as business associates of those healthcare providers. Compliance with the HIPAA standards was required as of April 14, 2003 for most entities. HITECH has different compliance dates with many sections of HITECH requiring compliance by February of 2010.

Enforcement – What Covered Entities Need to Know

The Office for Civil Rights ("OCR") is charged with responsibility for enforcing HIPAA. OCR seeks voluntary compliance but has power to impose significant civil monetary penalties for noncompliance. OCR may conduct compliance reviews and audits and investigate complaints alleging HIPAA violations. If OCR determines that a violation has occurred, OCR may impose a civil monetary penalty of up to $500,000 per violation up to a maximum of $1.5 million per year. OCR also works in conjunction with the Department of Justice (DOJ) to refer possible criminal violations of HIPAA.

- HITECH provides OCR with significant enhancements of its enforcement capabilities. It is anticipated that the number and intensity of OCR investigations of alleged HIPAA violations will greatly expand with the implementation of the HITECH provisions.

Following Federal and State Law

HITECH imposes breach notification requirements should health information be improperly disclosed. In many instances a breach requiring patient notification under HIPAA/HITECH will also trigger notification under state law.

- The following chart is intended to compare the similarities and differences between the HIPAA/HITECH and Idaho's data breach notification statute, and outlines the definitions and notification requirements under both federal and state law.

Comparison of the HIPAA/HITECH Act and Idaho's Data Breach Notification Statute.

TOPIC	HIPAA/HITECH[1]	IDAHO STATUTE
Effective Date for Rule Implementation	September 23, 2009	July 1, 2006 [2]
Government Enforcement Begins	HHS will not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 days from the date of publication of the HITECH rules. (August 24, 2009 through February 22, 2010).	July 1, 2006 [3]
Type of Information Covered	Unsecured protected health information ("PHI"). [4]	Unencrypted [5] computerized data containing personal information.[6]
Breach Notification Activator	Discovery of a breach of unsecured PHI. [7]	Notification is required if the investigation required by statute [8] determines that misuse of information about an Idaho resident has occurred or is reasonably likely to occur. [9] If the entity whose system was breached does not own or license the personal information at risk, the entity shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach, if misuse of personal information about an Idaho resident occurred or is reasonably likely to occur. [10]
Breach Definition	The acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI.[11]	Illegal acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information for one or more persons maintained by an agency, individual or a commercial entity.[12]

1. Refers to the Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). All section references below are to the HITECH Act.
2. 2006 Idaho Sess. Laws ch. 258.
3. 2006 Idaho Sess. Laws ch. 258.
4. "Unsecured protected health information" means "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary [of Health and Human Services] in guidance." § 13402(h). This guidance was issued on April 17, 2009 and is published in the Federal Register at 74 FR 19006.
5. What constitutes "encryption" or "encrypted data" is not defined by the statute. ICA §§ 28-51-104, 105.
6. "Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) social security number; (b) driver's license number or Idaho identification card number; or (c) account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. ICA § 28-51-104(5).ICA § 28-51-105(1).

TOPIC	HIPAA/HITECH	IDAHO STATUTE
Exceptions to Breach Definition	1. Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the covered entity or business associate if done in good faith and within the scope of authority granted and does not result in further use or disclosure in a manner not permitted under HIPAA. [13] 2. Inadvertent disclosure between persons authorized to have access by the same covered entity or business associate or organized health care arrangement and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.[14] 3. Disclosure of PHI where the covered entity or business associate has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the PHI. [15]	Good faith acquisition of personal information by an employee or agent of an agency, individual or a commercial entity for the purposes of the agency, individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. [16]
Direct Notification	Written notice by first-class mail to the individual at the last known address of the individual or, if the individual agreed to electronic notice, by electronic mail. [17]	May be provided by one of the following methods: 1. Written notice,[18] 2. Telephonic notice,[19] 3. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001. [20]

7. A breach is treated as "discovered" as of the first day on which the breach is known by the covered entity or, by exercising reasonable diligence would have been known to the covered entity. § 164.404.
8. Once an entity covered by the statute becomes aware of a breach, the entity is required to promptly conduct a good-faith reasonable investigation to determine the likelihood that personal information has been or will be misused. ICA § 28-515-105(1).§ 164.402 (2)(i).
9. ICA § 28-51-105(1).
10. ICA § 28-51-105(2).
11. "Compromises the security or privacy of the protected health information" means "poses a significant risk of financial, reputational, or other harm to the individual." § 164.402 (1)(i).
12. ICA § 28-51-104(2).
13. § 164.402 (2)(i).
14. § 164.402 (2)(ii).
15. §164.402 (2)(iii).
16. ICA § 28-51-104(2).

TOPIC	HIPAA/HITECH	IDAHO STATUTE
Substitute Notification—When Allowed	Allowed when there is insufficient or out-of-date contact information that precludes written notification.[21]	Allowed when there is insufficient contact information to provide the notice, or if the cost of providing the notice would exceed $250,000, or if the number of affected individuals exceeds 500,000.[22]
Substitute Notification—Method of Delivery	1. If fewer than 10 individuals are to be notified, substitute notice may be provided by an alternative form of written notice, telephone, or other means.[23] 2. If more than 10 individuals are to be notified, substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside.[24]	Substitute notice must include all of the following: 1. An electronic mail notice when the person or business has an electronic mail address for the subject persons; and Conspicuously posted in the website of the company responsible for the breach; and 2. Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and 3. Notice to major statewide media. [25]
Notification Deadlines	Notification is to be provided "without unreasonable delay and in no case later than 60 calendar days after discovery of the breach."[26]	Notification must be made "in the most expedient time possible and without unreasonable delay."[27]
Delay in Notification Allowed?	Allowed for 30 days if a law enforcement official states to the covered entity or business associate that notification would impede a criminal investigation or cause damage to national security. Delays of more than 30 days allowed only if law enforcement official makes a written request. [28]	Allowed if a law enforcement agency advises that the notification will impede a criminal investigation. [29]

17. § 164.404 (d)(1).
18. ICA § 28-51-104(4)(a).
19. ICA § 28-51-104(4)(b).
20. ICA § 28-51-104(4)(c).
21. § 164.404 (d)(2).
22. ICA § 28-51-104(4)(d).
23. § 164.404 (d)(2)(i).
24. For this substitute notice the covered entity must also establish a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured PHI may be included in the breach. § 164.404 (d)(2)(ii).
25. ICA § 28-51-104(4)(d).
26. § 164.404 (b).
27. ICA § 28-51-105(1). The statute permits the timing of the disclosure to vary "consistent with any measures necessary to determine the scope of the breach, to identify the individuals affected, and to restore the reasonable integrity of the computerized data system." ICA § 28-51-105(1).
28. § 164.412.
29. ICA § 28-51-105(3).
30. § 164.404 (c).
31. § 164.406.
32. § 164.408 (b).
33. § 164.408 (c).
34. ICA § 28-51-104(4)(d).

Comparison of the HIPAA/HITECH Act and Idaho's Data Breach Notification Statute.

TOPIC	HIPAA/HITECH	IDAHO STATUTE
Notification Information	1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; 2. A description of the types of PHI involved in the breach; 3. Steps individuals should take to protect themselves from potential harm resulting from the breach; 4. Brief description of what the covered entity is doing to investigate, mitigate, and protect against any further breaches; and 5. Contact procedures for individuals to ask questions or learn additional information which shall include a toll-free telephone number, an e-mail address, web site, or postal address.[30]	Not specified in the statute.
Notification to Media, Government and/or Third Parties	Media: If breach affects more than 500 residents of a state or jurisdiction.[31] Government-500 or More Affected: If breach affects 500 or more individuals, notice must be given to HHS contemporaneously with the notice being given to the affected individual.[32] Government-Fewer Than 500 Affected: If breach affects fewer than 500 individuals, covered entity shall maintain a log or other documentation of breaches and provide that information to HHS within 60 days after the end of each calendar year.[33]	Media: When substitute notice is permitted, e.g., when there is insufficient contact information to provide direct notice, or if the cost of providing direct notice would exceed $250,000, or if the number of affected individuals exceeds 500,000.[34]

Published January 2010

ID_V3_H

Healthcare Practice

Garvey Schubert Barer serves leading healthcare organizations across the Northwest, including hospitals, ambulatory surgery centers, managed care providers, long-term care facilities, physician organizations, clinical laboratory and pathology companies, genomic laboratories, medical device manufacturers, third-party payors, and healthcare associations. We understand the constraints facing the industry, and offer a wide range of services, including:

- Acquisitions, Consolidations, Mergers and Other Transactions
- Antitrust
- Bankruptcy
- Bond and Other Capital Financing
- Business and Corporate
- Federal and State Regulatory Advice
- Federal, State and Local Taxation
- Fraud and Abuse Regulation
- HIPAA
- Integrated Delivery Systems, Joint Ventures and Other Collaborative Arrangements
- IP and Technology
- Labor Relations and Employment Advice
- Litigation and Dispute Resolution
- Managed Care and Health Insurance
- Provider Reimbursement and RAC Audit Defense
- Quality Assurance
- Real Estate

We appreciate the economic, regulatory and competitive challenges facing the healthcare industry. Our goal is to partner with our clients, serving as trusted advisors to help our clients succeed in this competitive industry.

Garvey Schubert Barer

Garvey Schubert Barer is a full-service law firm with over 100 lawyers serving clients in the United States and abroad, with particular focus on the Pacific Northwest. From our five strategic locations, Beijing, New York, Portland, Seattle and Washington, D.C., we serve as outside counsel to established market leaders, newly launched enterprises and governmental bodies. Since its inception in 1966, GSB has served clients across virtually all industry sectors, including healthcare, technology, trade, transportation, maritime, financial services, real estate, communications and media, entertainment and manufacturing. The firm provides comprehensive, practical solutions to Fortune 500 companies and a broad range of privately held companies, investment firms, financial institutions, not-for-profit organizations and individuals.

Healthcare Practice

Stephen Rose
srose@gsblaw.com
206.464.3939 Ext 1375

Nancy Cooper
ncooper@gsblaw.com

Carla DewBerry
cdewberry@gsblaw.com

David Gee
dgee@gsblaw.com

Roger Hillman
rhillman@gsblaw.com

Eric Lindenauer
elindenauer@gsblaw.com

Lam Nguyen-Bull
hqnguyen@gsblaw.com

Emily Studebaker
estudebaker@gsblaw.com

Scott Warner
swarner@gsblaw.com

Portland

Bank of America Financial Center
121 SW Morrison Street
11th Floor
Portland, OR 97204-3141
503.228.3939 Tel
503.226.0259 Fax

Seattle

Second & Seneca Building
1191 Second Avenue
18th Floor
Seattle, WA 98101-2939
206.464.3939 Tel
206.464.0125 Fax