

HEALTHCARE PRACTICE

HIPAA/HITECH ACT vs.

OREGON CONSUMER IDENTITY THEFT
PROTECTION ACT

NOVEMBER 2009

G A R V E Y
S C H U B E R T
B A R E R

Attorneys



BEIJING NEW YORK PORTLAND SEATTLE WASHINGTON, D.C.

HEALTHCARE PRACTICE

STEPHEN ROSE

SROSE@GSBLAW.COM

206.464.3939 EXT 1375

LARRY BRANT

LBRANT@GSBLAW.COM

NANCY COOPER

NCOOPER@GSBLAW.COM

CARLA DEWBERRY

CDEWBERRY@GSBLAW.COM

JOY ELLIS

JELLIS@GSBLAW.COM

DAVID GEE

DGEE@GSBLAW.COM

ROGER HILLMAN

RHILLMAN@GSBLAW.COM

BENJAMIN LAMBIOTTE

BLAMBIOTTE@GSBLAW.COM

ERIC LINDENAUER

ELINDENAUER@GSBLAW.COM

LAM NGUYEN-BULL

HNGUYEN@GSBLAW.COM

THERESA SIMPSON

TSIMPSON@GSBLAW.COM

EMILY STUDEBAKER

ESTUDEBAKER@GSBLAW.COM

LOWELL TURNBULL

LTURNBULL@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 the Oregon Consumer Identity Theft Protection Act ("CITPA"), and outlines the definitions and notification requirements under both federal and state law.

COMPARISON OF THE HIPAA/HITECH ACT AND THE OREGON CONSUMER IDENTITY THEFT PROTECTION ACT (“CITPA”)

TOPIC	HIPAA/HITECH ¹	OREGON CITPA
Effective Date for Rule Implementation	September 23, 2009	2007
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. (Approximately August 24, 2009 through February 20, 2010).	2007
Type of Information Covered	Unsecured protected health information (“PHI”). ²	Unencrypted ³ computerized data containing personal information. ⁴
Breach Notification Activator	Discovery of a breach of unsecured PHI. ⁵	Discovery of a breach if the breach materially compromises the security, confidentiality or integrity of personal information.
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. ⁶	Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information. ⁷

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. “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.
3. “Encryption” means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key. ORS 646A.602 (6).
4. “Personal Information” means a consumer’s first name or first initial and last name in combination with any one or more of the following unencrypted data elements: (a) Social Security number; (b) Driver license number or state identification card number issued by the Oregon Department of Transportation; (c) Passport number or other United States identification card number; or (d) financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer’s financial account, or any of the unencrypted data elements or any combination of the data elements ((a) through (d)) not combined with the consumer’s first name or first initial and last name if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised. ORS 646A.628(11).
5. 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.
6. “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).
7. ORS 646A.602 (1)(a).

TOPIC	HIPAA/HITECH	OREGON CITPA
<p>Exceptions to Breach Definition</p>	<ol style="list-style-type: none"> 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.⁸ 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.⁹ 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.¹⁰ 	<p>Good-faith acquisition of personal information by an employee or agent for a legitimate purpose provided that the personal information is not used in violation of applicable laws or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.¹¹</p>
<p>Direct Notification</p>	<p>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.¹²</p>	<p>May be provided by one of the following methods:</p> <ol style="list-style-type: none"> 1. Written notice,¹³ or 2. Electronic notice if the customary method of communication with the consumer is by electronic means, or 3. Telephone notice provided the contact is made directly with the affected person.¹⁴
<p>Substitute Notification— When Allowed</p>	<p>Allowed when there is insufficient or out-of-date contact information that precludes written notification.¹⁵</p>	<p>Cost of providing notice would exceed \$250,000 and number of affected individuals exceeds 350,000 or if sufficient contact information for affected individuals is lacking.¹⁶</p>

8. § 164.402 (2)(i).

9. § 164.402 (2)(ii).

10. § 164.402 (2)(iii).

11. ORS 646A.602 (1)(b).

12. § 164.404 (d)(1).

13. The statute does not define the term “written notice.”

14. 14 ORS 646A.604 (4) (a)-(c).

15. 15 § 164.404 (d)(2).

16. 16 ORS 646A.604 (4)(d).

COMPARISON OF THE HIPAA/HITECH ACT AND THE OREGON
CONSUMER IDENTITY THEFT PROTECTION ACT (CITPA)

TOPIC	HIPAA/HITECH	OREGON CITPA
Substitute Notification— Method of Delivery	<ol style="list-style-type: none"> 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.¹⁷ 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.¹⁸ 	Conspicuous posting of the notice or a link to the notice on the Internet home page of the company responsible for the breach and notification to statewide television and newspaper media. ¹⁹
Notification Deadlines	Notification is to be provided “without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.” ²⁰	Immediately upon discovery of the breach. ²¹
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.	Allowed if a law enforcement agency determines that notification will impede a criminal investigation and the law enforcement agency makes a written request that notification be delayed. ²³
Notification Information	<ol style="list-style-type: none"> 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.²⁴ 	<ol style="list-style-type: none"> 1. A description of the incident in general terms; 2. The approximate date of the breach; 3. The type of personal information obtained as a result of the breach; 4. Contact information of company responsible for the breach; 5. Contact information for national consumer reporting agencies; and 6. Advice to affected individual on how to report suspected identity theft to law enforcement and the Federal Trade Commission.²⁵

17. § 164.404 (d)(2)(i).

18. 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).

19. ORS 646A.604 (4)(d) (A)-(B).

20. § 164.404 (b).

21. ORS 646A.604 (2).

22. § 164.412.

23. ORS 646A.604 (3).

24. § 164.404 (c).

25. AS 45.48.010 (a).

COMPARISON OF THE HIPAA/HITECH ACT AND THE OREGON CONSUMER IDENTITY THEFT PROTECTION ACT (CITPA)

TOPIC	HIPAA/HITECH	OREGON CITPA
Notification to Media, Government and/or Third Parties	<p><u>Media</u>: If breach affects more than 500 residents of a state or jurisdiction.²⁶</p> <p><u>Government-500 or More Affected</u>: If breach affects 500 or more individuals, notice must be given to HHS contemporaneously with the notice being given to the affected individual.²⁷</p> <p><u>Government-Fewer Than 500 Affected</u>: 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.²⁸</p>	If breach affects more than 1,000 individuals notice must be given to all consumer reporting agencies ²⁹ that compile and maintain reports on consumers on a nationwide basis. ³⁰

26. § 164.406.

27. § 164.408 (b).

28. § 164.408 (c).

29. "Consumer reporting agency" means a consumer reporting agency as described in the federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)) as that Act existed on October 1, 2007. ORS 646A.602 (4).

30. ORS 646A.604 (6).

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

LARRY BRANT
LBRANT@GSBLAW.COM

NANCY COOPER
NCOOPER@GSBLAW.COM

CARLA DEWBERRY
CDEWBERRY@GSBLAW.COM

JOY ELLIS
JELLIS@GSBLAW.COM

DAVID GEE
DGEE@GSBLAW.COM

ROGER HILLMAN
RHILLMAN@GSBLAW.COM

BENJAMIN LAMBIOTTE
BLAMBIOTTE@GSBLAW.COM

ERIC LINDENAUER
ELINDENAUER@GSBLAW.COM

LAM NGUYEN-BULL
HONGUYEN@GSBLAW.COM

THERESA SIMPSON
TSIMPSON@GSBLAW.COM

EMILY STUDEBAKER
ESTUDEBAKER@GSBLAW.COM

LOWELL TURNBULL
LTURNBULL@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