GARVEY SCHUBERT BARER

HEALTHCARE PRACTICE

Breach Notification Requirements Under HIPAA/HITECH Act and Oregon Consumer Identity Theft Protection Act

OREGON

AUGUST 2013

ANCHORAGE BEIJING NEW YORK PORTLAND SEATTLE WASHINGTON, D.C.

www.GSBLaw.com

Healthcare Practice

Stephen Rose
srose@gsblaw.com
206.816.1375
907.258.2400

Kathryn Ball
kball@gsblaw.com
503.553.3104

Larry Brant
lbrant@gsblaw.com
503.553.3114

Nancy Cooper
ncooper@gsblaw.com
503.553.3174

Joy Ellis
jellis@gsblaw.com
503.553.3121

Roger Hillman
rhillman@gsblaw.com
206.816.1402

Sandy Johnson
stjohnson@gsblaw.com
206.816.1349

Eric Lindenauer
elindenauer@gsblaw.com
503.553.3117

Barbra Nault
bnault@gsblaw.com
907.258.2400

Theresa Simpson
tsimpson@gsblaw.com
206.816.1425

Emily Studebaker
estudebaker@gsblaw.com
206.816.1417

Scott Warner
swarner@gsblaw.com
206.816.1319

HIPAA/HITECH/OMNIBUS RULE BACKGROUND

In 2003, compliance with the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Regulations became mandatory. The purpose of HIPAA is to provide baseline federal protections for protected health information ('PHI") 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 more severe enforcement penalties and details notification requirements to patients should their health information be improperly disclosed. In 2013, HIPAA/HITECH was supplemented by what is now called the HIPAA Omnibus Rules, 78 Fed. Reg. 5566 (January 25, 2013). In short, the HIPAA/HITECH/ Omnibus Rules affect a very wide range of healthcare providers, from hospitals, doctors, chiropractors, and nursing homes, to pharmacies and health plan providers, as well as business associates of those healthcare providers.

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 money 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 money penalty of up to $50,000 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.

- The Omnibus Rule 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 Omnibus Rule provisions.

FOLLOWING FEDERAL AND STATE LAW

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

- The following chart is intended to compare the similarities and differences between the HIPAA/HITECH/Omnibus Rule 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	Oregon CITPA
Effective Date for Rule Implementation	September 23, 2009	2007
Government Enforcement Begins	HHS will not impose sanctions for failure to comply with the HIPAA Omnibus Rule, 78 Fed. Reg. 5566 (January 23, 2013), until September 23, 2013.*	2007
Type of Information Covered	Unsecured protected health information ("PHI").[1]	Unencrypted[2] computerized data containing personal information.[3]
Breach Notification Activator	Discovery of a breach of unsecured PHI.[4]	Discovery of a breach or notification of a breach from any person that maintains or otherwise possesses personal information on behalf of the owner or licensor.[5]
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]	An unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information that a person maintains.[7]

1. "Unsecured protected health information" means "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary [of Health and Human Services] in guidance." § 164.402(2). This guidance was issued on April 17, 2009 and is published in the Federal Register at 74 Fed. Reg. 19006.
2. "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).
3. "Personal information" means a consumer's first name or first initial and last name in combination with any one of the following unencrypted data elements: (a) social security number; (b) driver's license number or state identification card number issued by the Oregon Department of Transportation; (c) passport number or other United States issued identification 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. ORS 646A.602(11).
4. 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(a)(2).
5. ORS 646A.604(1)-(2).
6. The acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA is presumed to be a breach unless the incident fits into one of the three Exceptions to Breach Definition or the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment. § 164.404(a)(2).
7. ORS 646A.602(1)(a).

* NOTE: A separate enforcement date applies to Business Associate Agreements.

Comparison of the HIPAA/HITECH Act and the Oregon Consumer Identity Theft Protection Act ("CITPA")

Topic	HIPAA/HITECH	Oregon CITPA
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.[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]	A good faith acquisition of personal information by an employee or agent is not a breach 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]
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.[12]	May be provided by one of the following methods: 1. Written notice;[13] or 2. Electronic notice, if the customary method of communication with the consumer is by electronic means or is consistent with the provisions regarding electronic records and signatures set forth in the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001) as that act existed on October 1, 2007; or 3. Telephone notice provided the contact is made directly with the affected person.[14]

8. § 164.402(1)(i).
9. § 164.402(1)(ii).
10. § 164.402(1)(iii).
11. ORS 646A.602(1)(b).
12. § 164.404(d)(1).
13. The statute does not define "written notice."
14. ORS 646A.604(4)(a)-(c).

Comparison of the HIPAA/HITECH Act and the Oregon Consumer Identity Theft Protection Act ("CITPA")

Topic	HIPAA/HITECH	Oregon CITPA
Substitute Notification - When Allowed	Allowed when there is insufficient or out-of-date contact information that precludes written notification.[15]	Allowed when cost of providing notice would exceed $250,000, the number of affected individuals exceeds 350,000, or if sufficient contact information for affected individuals is lacking.[16]
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.[17] 2. If 10 or more 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 website 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.[22]	Allowed if a law enforcement agency determines that notification will impede a criminal investigation and makes a written request that notification be delayed.[23]

15. § 164.404(d)(2).
16. ORS 646A.604(4)(d).
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)(B).
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).

Comparison of the HIPAA/HITECH Act and the Oregon Consumer Identity Theft Protection Act ("CITPA")

Topic	HIPAA/HITECH	Oregon CITPA
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 unsecured PHI involved in the breach; 3. Steps individuals should take to protect themselves from potential harm resulting from the breach; 4. A 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 email address, website, or postal address.[24]	1. A description of the incident in general terms; 2. The appropriate 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]
Notification to Media, Government and/or Third Parties	**Media**: If breach affects more than 500 residents of a state or jurisdiction.[26] **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.[27] **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.[28]	**Media**: If cost of providing notice would exceed $250,000, the number of affected individuals exceeds 350,000, or if sufficient contact information for affected individuals is lacking.[29] **Consumer Credit Reporting Agencies**: If breach affects more than 1,000 individuals, notice must be given to all consumer reporting agencies[30] that compile and maintain reports on consumers on a nationwide basis.[31]

24. § 164.404(c).
25. ORS 646A.604(5)(a)-(f).
26. § 164.406(a).
27. § 164.408(b).
28. § 164.408(c).
29. ORS 646A.604(4)(d)(B).
30. "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).
31. 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, medical device manufacturers, third-party payors, and healthcare associations. We 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 Defense
- Government Audit Defense
- 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
- Real Estate
- Risk Management

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 six strategic locations, Anchorage, 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
206.816.1375
907.258.2400

Kathryn Ball
kball@gsblaw.com
503.553.3104

Larry Brant
lbrant@gsblaw.com
503.553.3114

Nancy Cooper
ncooper@gsblaw.com
503.553.3174

Joy Ellis
jellis@gsblaw.com
503.553.3121

Roger Hillman
rhillman@gsblaw.com
206.816.1402

Sandy Johnson
stjohnson@gsblaw.com
206.816.1349

Eric Lindenauer
elindenauer@gsblaw.com
503.553.3117

Barbra Nault
bnault@gsblaw.com
907.258.2400

Theresa Simpson
tsimpson@gsblaw.com
206.816.1425

Emily Studebaker
estudebaker@gsblaw.com
206.816.1417

Scott Warner
swarner@gsblaw.com
206.816.1319

GARVEY SCHUBERT BARER

Anchorage
2550 Denali Street
Suite 1502
Anchorage, AK 99503
907.258.2400 Tel
907.258.2401 Fax

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

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

Anchorage Beijing New York Portland Seattle Washington, D.C.

www.GSBLaw.com