



**GARVEY
SCHUBERT
BARER**

HEALTHCARE PRACTICE

Breach Notification Requirements Under
HIPAA/HITECH Act
and
Alaska Personal Information Protection Act



ALASKA

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

Barbra Nault

bnault@gsblaw.com
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

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 Alaska Personal Information Protection Act ("PIPA"), and outlines the definitions and notification requirements under both federal and state law.

COMPARISON OF THE HIPAA/HITECH ACT AND THE ALASKA PERSONAL INFORMATION PROTECTION ACT (“PIPA”)

TOPIC	HIPAA/HITECH	ALASKA PIPA
Effective Date for Rule Implementation	September 23, 2009	July 1, 2009
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.*	July 1, 2009
Type of Information Covered	Unsecured protected health information (“PHI”). ¹	Personal Information. ²
Breach Notification Activator	Discovery of a breach of unsecured PHI. ³	Discovery of a breach or being notified of a breach and there is a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. ⁴
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. ⁵	Unauthorized acquisition ⁶ , or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information. 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. “Personal Information” means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of (A) an individual’s name (either first name or first initial and last name) and (B) one or more of the following data elements: (i) social security number; (ii) driver’s license number or state identification card; (iii) account number, credit card number, or debit card number with access code(s) or personal identification number; (iv) passwords, personal identification numbers, or other access codes for financial accounts. AS 45.48.090(7).
3. 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).
4. Disclosure of the breach to the consumer is not required if, after an appropriate investigation and after written notification to the attorney general, it is determined that there is not a reasonable likelihood that harm to the consumer will result. AS 45.48.010.
5. 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 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).
6. “Acquisition” includes acquisition by photocopying, facsimile, or other paper-based method or acquisition by a device, including a computer, that can read, write, or store information that is represented in numerical form, or any other method. AS 45.48.090(1)(A)-(C).
7. AS 45.48.090(1).

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

COMPARISON OF THE HIPAA/HITECH ACT AND THE ALASKA PERSONAL INFORMATION PROTECTION ACT (“PIPA”)

TOPIC	HIPAA/HITECH	ALASKA PIPA
Exceptions to Breach Definition	<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 	Breach excludes the good faith acquisition of personal information by an employee or agent for a legitimate purpose provided that the employee or agent does not use the personal information for a purpose unrelated to a legitimate purpose and does not make any further unauthorized disclosure 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	<ol style="list-style-type: none"> 1. Notice by written document sent to the most recent address for the affected individual; or 2. Notice by electronic means: <ol style="list-style-type: none"> A. If the primary method of communication with the affected individual has been by electronic means, or B. If making the disclosure by electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act).¹³

8. § 164.402(1)(i).

9. § 164.402(1)(ii).

10. § 164.402(1)(iii).

11. AS 45.48.050.

4

12. § 164.404(d)(1).

13. AS 45.48.030(1) and (2).

COMPARISON OF THE HIPAA/HITECH ACT AND THE ALASKA PERSONAL INFORMATION PROTECTION ACT (“PIPA”)

TOPIC	HIPAA/HITECH	ALASKA PIPA
Substitute Notification - When Allowed	Allowed when there is insufficient or out-of-date contact information that precludes written notification. ¹⁴	Allowed when there is insufficient contact information to provide the notice, or if the cost of providing notice would exceed \$150,000, or if the number of affected individuals exceeds 300,000. ¹⁵
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.¹⁶ 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.¹⁷ 	Notice is to be: <ol style="list-style-type: none"> 1. Sent by email if affected individual’s email address is known; 2. Conspicuously posted in the website of the company responsible for the breach; and 3. Provided to major statewide media.¹⁸
Notification Deadlines	Notification is to be provided “without unreasonable delay and in no case later than 60 calendar days after discovery of the breach.” ¹⁹	Notification to be provided “in the most expeditious time possible and without unreasonable delay. . . .” ²⁰
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. ²¹	Allowed if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. ²²

14. § 164.404(d)(2).

15. AS 45.48.030(3).

16. § 164.404(d)(2)(i).

17. 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).

18. AS 45.48.030(3).

19. § 164.404(b).

20. AS 45.48.010(b).

21. § 164.412.

22. AS 45.48.020.

COMPARISON OF THE HIPAA/HITECH ACT AND THE ALASKA PERSONAL INFORMATION PROTECTION ACT (“PIPA”)

TOPIC	HIPAA/HITECH	ALASKA PIPA
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 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.²³ 	Entity causing the breach is directed to “disclose the breach to each state resident whose personal information was subject to the breach.” ²⁴
Notification to Media, Government and/or Third Parties	<p>Media: If breach affects more than 500 residents of a state or jurisdiction.²⁵</p> <p>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.²⁶</p> <p>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.²⁷</p>	<p>Media: If cost of breach notification would exceed \$150,000 or if 300,000 state residents affected.²⁸</p> <p>Government: If breaching party believes breach does not pose a reasonable likelihood of harm to the affected individuals, breaching party is to document said determination, notify state attorney general, and maintain documentation of this determination for five years.²⁹</p> <p>Consumer Credit Reporting Agencies: If more than 1,000 state residents are required to be notified of a breach, the breaching party must also notify, without unreasonable delay, all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis.</p>

23. § 164.404(c).

24. AS 45.48.010(a).

25. § 164.406(a).

26. § 164.408(b).

27. § 164.408(c).

28. AS 45.48.030(3).

29. AS 45.48.010(c).

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

Barbra Nault

bnault@gsblaw.com
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

Theresa Simpson

tsimpson@gsblaw.com
206.816.1425

Emily Studebaker

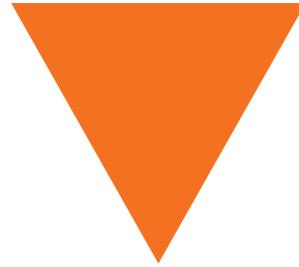
estudebaker@gsblaw.com
206.816.1417

Scott Warner

swarner@gsblaw.com
206.816.1319



**GARVEY
SCHUBERT
BARER**



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

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

ANCHORAGE

BEIJING

NEW YORK

PORTLAND

SEATTLE

WASHINGTON, D.C.

www.GSBLaw.com