

# SecureGRC SB™ Whitepaper

**Keep your Healthcare business...  
Secure and Healthy!**



**Check your Security and Compliance Status**



The SecureGRC SB™ way!





## Disclaimer

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, EGESTALT TECHNOLOGIES INC. PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of eGestalt Technologies, Inc., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of authorized personnel eGestalt Technologies Inc. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

Information about and around HIPAA and HITECH continues to evolve and the information here are subject to change. This information is provided as is without warranty

While every effort has been made to insure that the information presented is correct, but we cannot offer such assurances.

HIPAA /HITECH rules and regulations are subject to lots of different interpretations and this is subjective.

You should not rely on this information for auditing or legal purposes, but simply use it as a means to raise your awareness.

We are not attorneys! Consult with your own legal counsel, auditors or advisors.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Changes or improvements may be made to the software described in this document at any time.

© 2010 eGestalt Technologies Inc., all rights reserved.



## CONTENT OUTLINE

In this White Paper .....	5
PHI .....	6
What is HIPAA? .....	6
What is HITECH? And Why Should I, a Healthcare-provider, Care? .....	6
Penalties and Expanded Enforcement .....	7
There's Security and then there's Compliance .....	8
How Can You Protect Your Business? .....	8
SecureGRC SB from eGestalt .....	8
Simplify the complex and time consuming process of getting into and maintaining Compliance. ....	9
Cloud-Delivered .....	9
Simple Self-Assessment Tools .....	9
Built-in Best Practices .....	9
Key Advantages of SecureGRC SB from eGestalt: .....	9
SecureGRC SB Client Case Studies .....	9



---

## Keep Your Healthcare Business Secure and Compliant!

---



From HealthCareInfoSecurity.com...

**February 23, 2011** – “For the first time, federal officials have fined a healthcare organization for violations of the HIPAA privacy rule. Cignet Health of Prince George's County, Md., was **fined \$4.3 million** for the violations that involved failing to provide 41 patients with access to their medical records and then failing to cooperate with federal investigators. Cignet, a Christian-influenced medical service, operates four clinics in southern Maryland. The HITECH Act created higher fines for HIPAA violations, which were issued in this case. **"The U.S. Department of Health and Human Services is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule,"** said HHS Secretary Kathleen Sebelius.”

**February 24, 2011** – “In the second major HIPAA enforcement action announced by federal authorities this week, Massachusetts General Hospital and its physicians organization have entered into a resolution agreement that calls for **paying a \$1 million settlement** and taking corrective action to avoid future violations. The case involved the loss of documents that included information on patients with HIV/AIDS. The resolution agreement with Massachusetts General stems from the loss of scheduling documents for 192 patients in the hospital's General Infections Disease Associates outpatient practice, including those with HIV/AIDS. OCR initiated its investigation when a patient whose information was lost filed a complaint.”

“With the two announcements of penalties for HIPAA privacy rule violations, HHS' Office for Civil Rights appears to be giving strong signals that its long-promised plans to ramp up enforcement efforts are now a reality.” “We hope the healthcare industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement,” said OCR Director Georgina Verdugo.”

There is no question that the increasing frequency and severity of violations is causing a dramatic increase in HIPAA/HITECH enforcement and penalties by the HHS and related agencies.

### Frightening?

You should be frightened!! The fact is that healthcare regulatory requirements are no longer just for healthcare providers. If you are a Business Associate to a healthcare provider and that brings you in contact with Protected Health Information (PHI) you too are subject to regulatory acts such as HIPAA and HITECH, and liable for some substantial penalties if you do not maintain compliance! You need to take this seriously.



## In this White Paper

In this white paper we'll bring you fully up to speed on exactly what the implications of HIPAA & HITECH regulations are and what it means for your business. If you are a healthcare provider, covered entity (CE) or a business associate (BA), the paper provides details on what your potential security and compliance exposures could be. We will also introduce you to SecureGRC SB™ from eGestalt technologies Inc, a set of powerful, yet simple-to-use, Cloud-based, Software-as-a-Service (SaaS) delivered solution that will help you assess your risk, analyze and mitigate your risk exposure and move towards continuous HIPAA/HITECH security and compliance!



## PHI

Protected Health Information (PHI) includes any data, including demographic information that relates to:

- The individual's past, present or future physical or mental health or condition,
- The provision of health care to the individual, or
- The past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.
- Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number)

## What is HIPAA?

Perhaps the most often misspelled acronym in all of public regulatory jargon, HIPAA (not HIPPA) is the Health Information Portability and Accountability Act. The official description:

***"Public Law 104-191, 104th Congress --An Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes."***

While most people think the "P" in HIPAA stands for "Privacy" it actually focuses the primary goal of the act which is to promote accountability for patient health information while in transit between various healthcare organizations and bodies. The assured portability of healthcare information plays a tremendous role in improving the safety, efficiency and quality of healthcare. The act seeks to assure that anyone and everyone who participates in moving PHI from place to place accepts accountability which, at least in part, assures privacy.

Many people are often confused into thinking that specific products, such as Information Technology products, are "HIPAA-certified" when in fact, they cannot be. HIPAA certification applies only to healthcare organizations and their operating facilities and processes. Products may enable or contribute to enabling HIPAA-compliance. As an example, a camera deployed to sense when a healthcare worker has left an information station and automatically logs them off contributes to achieving compliance with specific HIPAA rules surrounding logoff policies and procedures, but the camera itself is not "HIPAA-compliant."

The bottom line is that accountability for patient information is not just a compliance concern; it's a very real security concern as well! Hackers ARE going after patient data because they can sell it and make serious money. And if you let them, you may be liable to pay serious money in fines as well!!

## What is HITECH? And Why Should I, a Healthcare-provider, Care?

In February of 2009 when President Obama signed the American Recovery and Reinvestment Act (the "stimulus package") into law, it contained and enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act as well. This act has the effect of expanding the reach and impact of HIPAA, and most importantly the penalties contained within.

What is meant when we say that it "expanded the reach and impact" is that the HIPAA/HITECH law now not only applies to healthcare providers, referred to in the Act as "Covered Entities", medical providers who offer medical services to end-customers, but also to any Business Associate that shares protected health information with them.





A covered entity could be any of the following entities, who transmit information in electronic form for which HHS has adopted a standard, including the following:

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
<p>This includes providers such as:</p> <ul style="list-style-type: none"> <li>•Doctors</li> <li>•Clinics</li> <li>•Psychologists</li> <li>•Dentists</li> <li>•Chiropractors</li> <li>•Nursing Homes</li> <li>•Pharmacies</li> </ul> <p>...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.</p>	<p>This includes:</p> <ul style="list-style-type: none"> <li>•Health insurance companies</li> <li>•HMOs</li> <li>•Company health plans</li> <li>•Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs</li> </ul>	<p>This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.</p>

Business associates, which are now completely in scope, includes:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involves access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.
- Etc.

The law extends not only to companies, CE's and BA's, but also to *individuals who work within them*, making everyone who touches protected health information personally accountable for their actions, and exposed to potential penalties.

Business Associates who routinely exchange or access PHI of any Covered Entity may be subject to all the same privacy and security rules as the Covered Entity itself. The Act requires them to develop and implement comprehensive written PHI security policies and procedures, and makes provisions for audit of all Business Associates by the Health & Human Services department. Failure to comply can easily incur penalties. Also, the Act requires breach notification to patients, the HHS (health and human services), even major public media.

## Penalties and Expanded Enforcement

The HIPAA/HITECH Act carries serious implications for anyone who fails to achieve and maintain compliance. Civil Monetary Penalties include:



- **Where disclosure was unintentional or inadvertent, at least \$100, but no more than \$25,000, for each such violation**
- **Where there was "reasonable cause," but no willful neglect, at least \$1,000, but no more than \$100,000, for each such violation**
- **If there was willful neglect but the violation is corrected, at least \$10,000, but no more than \$250,000, for each such violation**
- **If there was willful neglect and the violation is not corrected, at least \$50,000 for each violation but no more than \$1,500,000**

The monetary penalties are substantial, and there are further ramifications potentially including imprisonment for overt or repeat offenders.

## There's Security and then there's Compliance

In their white paper "Compliance Does Not Equal Security," the leading security consultants at Lares point out that

*"The fact is that regulatory legislation was never written specifically to address the issue of network or data security. Guideline documentation for legislation such as HIPAA barely even mentions security at all. Yet many executives, whether guided by their IT management or their own misperceptions, continue to believe that achieving one automatically assures the other. This is not the case."*

*"While "regulatory compliance" can easily be defined as properly answering the questions and fulfilling the requirements of a given published set of requirements, security must be defined as having the sense that all of your assets are protected from compromise or theft to a level appropriate to the value of each asset. Regulatory Compliance is black & white, while security always exists in varying shades of grey."*

## How Can You Protect Your Business?



Bring in security + compliance protection. Compliance regulations are best security practices that need to be adopted.

Begin by recognizing that all the "deadlines" for compliance are now in the past. If you are a Covered Entity or a Business Associate of a Covered Entity, you need to achieve and maintain compliance now. If you interact directly with Covered Entities and exchange any patient data with them it is likely that the data is classified as Protected Health Information, making you a Business Associate, requiring you to achieve and maintain compliance.

Next, identify a reliable toolset for self-examination and self-audit to assure yourself that you will readily pass any HIPAA or HITECH audit that may be conducted by the HHS.

One reliable solution that small healthcare facilities find very helpful in supporting their self-examination is SecureGRC SB from eGestalt.

## SecureGRC SB from eGestalt

SecureGRC SB is a simple, cost-effective, easy-to-use security and compliance self-assessment solution, targeted at small-medium businesses, to help you understand and gain control over your HIPAA/HITECH requirements. It is constantly kept up to date with the latest versions and revisions.

Since SecureGRC SB is a Cloud-Delivered Software as a service (SaaS) solution, there are no hardware or software investments for you to worry about. Also, implementation is immediate and there are no support or backup requirements. Best of all, you enjoy the assurance that your compliance solution is future-proof!

Comprehensive HIPAA & HITECH support is built-in, easily extended, and automatically kept up to date. All data is stored in eGestalt's SaS 70 Type II secure Data Center and



NO e-PHI is ever removed from a client site. Your security and compliance support application is fully secure and compliant!

## **Simplify the complex and time consuming process of getting into and maintaining Compliance.**

Achieving regulatory compliance is really just a beginning. Maintaining continuous compliance is the key to mitigating risk, reducing exposure, and assuring avoidance of the increasing threat of penalties.

SecureGRC SB demystifies security and compliance through automation of the self-assessments you need to conduct in order to accomplish this.

## **Cloud-Delivered**

Because SecureGRC SB is cloud-delivered you don't engender any delay or make any new investments in new infrastructure. You simply access the web-interface to begin the comprehensive self-assessment processes.

## **Simple Self-Assessment Tools**

Start with question number 1, then 2. Just that simple. Once you have made your first pass, SecureGRC SB's unique risk calculator will help prioritize the areas you need to focus on first.

## **Built-in Best Practices**

With its built-in "Best Practices" library, extensive online help and documentation, SecureGRC SB explains how to resolve each and every open issue with a common sense approach.

## **Key Advantages of SecureGRC SB from eGestalt:**

- Peace of Mind
- Support for HIPAA & HITECH regulations.
- Simple, menu driven assessment to understand and gain control over your HIPAA/HITECH requirements
- Easy plug in if you also need PCI-DSS compliance
- Library of free policies and procedure templates to customize and then attach as evidence
- Also covers the Privacy and Security rules
- Tracking and managing of your Business Associates (BA's)
- Central repository for all your HIPAA related documentation
- A finished document that can be used to show compliancy to other organizations and auditors
- Automatic updates on new or revised policies, procedures, or forms which reflect changes in the standards
- Automatic updates to changes in regulatory requirements

## **SecureGRC SB Client Case Studies**

Here are just two examples, one a Covered Entity and the other a Business Associate, who have successfully employed SecureGRC SB to aid them in becoming and maintaining compliance.

"As a firm we had a policy of preparing non-disclosure agreements for all our clients. We thought this would cover us for HIPAA compliance as well, however we realized that with the new changes in the HITECH law, we needed to have a specific Business Associate Agreement in place with all of our medical clients and to show them that we are in fact HIPAA/HITECH compliant as well."



“We did some research online and found most programs to help get us complaint were in excess of \$10,000 and we were considering this when we discovered SecureGRC SB. This was a \$500 entry-point online service that was easy to use and provided us with an excellent tool to help us identify what we needed to do to become compliant. Once we completed their assessment, we received an easy-to-grasp report that we can use to demonstrate that we are now HIPAA and HITECH compliant.”

**Stephan C. Chait, CPA/ABV**

“I have been practicing for over 10 years and never thought I had any reason to be HIPAA compliant. After all, I have a private practice, I’m, not a hospital. But I attended a webinar by eGestalt on their product called SecureGRC SB. I quickly realized that I had several areas of exposure regarding my patient’s information. So I tried the SecureGRC SB program, as it was only \$500 and was easy to use.”

“I was really surprised in the number of areas that I was exposed. Using the program I quickly identified and fixed the problems. I am now requiring all of my Business Associates to use this program to help protect my practice. I know I would never get audited, that was not my concern. I just wanted to make sure I was doing the right things to protect my patient’s privacy and this was an inexpensive and low risk approach.”

**Dr. Ari J. Kellner - Mount Kisco, NY**

--XXXX--

---

#### **About eGestalt Technologies Inc.:**

eGestalt Technologies <<http://www.egestalt.com>> is a world-class, innovation driven, leading provider of cloud-computing based business solutions for information security and IT-GRC management. eGestalt is headquartered in Santa Clara, California, and has offices in US, Asia-Pacific and Middle East. eGestalt was nominated Breakthrough Technology Vendor at XChange Americas, August, 2010, and selected by SiliconIndia among the “Top 10 Security Companies to Watch”. The flagship product SecureGRC application was voted runner-up in the Managed Services Category at Xchange Tech Innovators, Nov. 2010.

To learn more about SecureGRC and SecureGRC SB versions from eGestalt and how it can help you protect your healthcare-related organization, visit <http://www.egestalt.com>, call us at **+1-(408)-689-2586**, or email at <mailto:sales@egestalt.com>.

---