A White Paper for HIPAA Business Associates (And Agents & Subcontractors!)

Preparing for the HIPAA Security Rule Again; now, with Teeth from the HITECH Act!

Introduction

Two years ago we first published "A White Paper for Health Care Professionals: Preparing for the HIPAA Security Rule" that was written for Covered Entities (CEs). This new paper updates that very popular original guide with a specific focus on what the HIPAA regulations define as a Business Associate (BA).

The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, significantly modified and strengthened many aspects of the HIPAA Security Rule, including the penalties that the HHS could impose for violations of the HIPAA rules.

The HIPAA Privacy and Security Rules obligate CEs and BAs to share Protected Health Information (PHI) with vendors if and only if assurances have been received that these vendors will safeguard the information:

> **The HIPAA Privacy Rule at 45 C.F.R. §164.504 Uses and disclosures:**
> Organizational requirements. (e)(1) Standard: Business associate contracts. …
> **(e) (2) Implementation specifications: Business associate contracts.** A contract between the covered entity and a business associate must:
> - (i) Establish the permitted and required uses and disclosures of such information by the business associate. …
> - (ii) Provide that the business associate will:
>
> (A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;
> (B) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
> (C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
> (D) Ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
>
> **The HIPAA Security Rule at 45 C.F.R. §164.308 Administrative Safeguards.**
> (b)(1) *Standard: Business associate contracts and other arrangements.* A covered entity, in accordance with §164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf **only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a) that the business associate will appropriately safeguard the information.**

The HIPAA Security Rule at 45 C.F.R. § 164.314 Organizational requirements details some of these specific terms and conditions.

With these Standards and Implementation Specifications, the regulations effectively create a "chain of trust" or "chain of custody" between the CE, its downstream BAs and the BAs' downstream Agents and Subcontractors.

It's time to get serious! After essentially ignoring the regulation for five years, Covered Entities and, now, BAs need to get serious! The deadline for BAs of Covered Entities to become fully compliant with relevant sections of the HIPAA Privacy and Security Rules and the HITECH Breach Notification Rule was February 17, 2010.

Benefit from our expertise – complete a HIPAA Security Rule refresher, learn about the sweeping changes to HIPAA overall and the Security Rule and Contingency Planning, in particular, and jump-start your Security Rule compliance efforts with our specific guidance.

As a reminder, the Health Insurance Portability and Accountability Act (HIPAA) comprises three sets of standards — transactions and code sets, privacy, and security. The goals of these standards are to:

- Simplify the administration of health insurance claims and lower costs.
- Give individuals more control over and access to their medical information.
- Protect individually identifiable medical information from threats of loss or disclosure.

The HIPAA Security Final Rule, the last of the three HIPAA Rules, was published in the February 20, 2003 Federal Register with an effective date of April 21, 2003. Most Covered Entities (CEs) had two full years -- until April 21, 2005 -- to comply with these standards. Many covered entities, especially providers, did not comply by that date and are still non-compliant. Now, millions more organizations (the BAs and their downstream Agents and Subcontractors) are now in this position… not compliant with the HIPAA and HITECH Rules.

In general, the Security Rule protects electronic patient health information (ePHI) whether it is stored in a computer or printed from a computer.

The HIPAA Security Rule is comprehensive including 22 standards defining with what safeguards those covered by the Rule must implement and 50+ implementation specifications that describe how the standards must be implemented. The documentation requirements for the Security Rule are daunting. In fact, there are two standards in the Rule covering policies and procedures and documentation. In some cases, no guidance is provided for how the standards must be implemented.

While this White Paper is focused on the Security rule, it is important to note that BAs are statutorily obligated to comply with relevant sections of the HIPAA Privacy Rule and HITECH Breach Notification Rule. The HIPAA Privacy Rule is even more comprehensive and complicated than the Security Rule, with 56 standards and 54 very "dense" implementation specifications. And to round out the three HIPAA-HITECH regulatory pillars, the Breach Notification Rule contains 4 standards and 9 implementation specifications.

To make matters worse, most Covered Entities and BAs covered by the Rules had and still have limited staff resources to implement an initiative to comply with the Security Rule. And available information security consulting expertise in many communities may be limited and expensive. The upshot has been: very poor information security in the healthcare industry.

Enter the HITECH Act which many describe as a "game-changer" and "ground-breaking". Many accurately observe that healthcare industry woefully unprepared for major changes in fifteen (15) key areas. Without a doubt, HITECH is the largest and most consequential expansion and change to the federal privacy and security rules ever. The fifteen (15) change areas comprise new federal privacy and security provisions that will have major financial, operational and legal consequences for all hospitals, medical practices, health plans, and now their "BAs," and some vendors and service providers that were not previously considered "BAs."

This white paper, presented in the form of Frequently Asked Questions, will help you prepare for the original sweeping changes in the way you must do business under the terms of the HIPAA Security Rule and includes specific updates to the Security Rule required by the HITECH Act.

Frequently Asked Questions about the HIPAA Security Rule and HITECH

Q1. Why do I need to be HIPAA Security compliant?

The HIPAA law requires all health care CEs and their BAs to safeguard the privacy of patient health information. The HIPAA law also requires CEs and BAs to implement required security measures to protect patient health information.

Q2. What is a "Covered Entity?"

Covered Entities (CEs) include all health care providers (doctors, dentists, therapists, psychologists, pharmacists, etc.), health care clearinghouses, and health plans (i.e., health insurance companies) that electronically store, process or transmit electronic protected health information (ePHI).

Previously, any BA of these CEs who by agreement has access to this ePHI was required to comply with the Security Rule as well by means of a so-called BA Agreement. The HITECH Act now explicitly places the same comprehensive Security Rule requirements on BAs to ensure that the same level of security is consistent throughout whenever health information is accessed or exchanged between organizations.

Q3. What is a "Business Associate?"

A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE. A member of the CE's workforce is not a BA.

A covered health care provider, health plan, or health care clearinghouse can be a BA of another CE. The Privacy Rule lists some of the functions or activities, as well as the particular services that make a person or entity a BA, if the activity or service involves the use or disclosure of PHI. The types of functions or activities that may make a person or entity a BA include payment or health

care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules.

Q4. What are some examples of BA services?

BA functions and activities include but are not limited to: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. BA services are: legal; actuarial; accounting; consulting; data aggregation; technology management; administrative; accreditation; and financial.

Q5. What are some examples of BAs?

- A Software-as-a-Service electronic health record (EHR) system provider.
- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to PHI.
- An attorney whose legal services to a health plan or provider involve access to PHI.
- 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.

Q6. What are the objectives of the HIPAA Security Rule?

The objectives of these rules are to:

- Ensure confidentiality, integrity, and availability of all ePHI that a CE or CE BA creates, receives, maintains, or transmits.

- Protect against any reasonably anticipated threats or hazards to the security or integrity of such ePHI.

- Protect against any reasonably anticipated losses or disclosures of ePHI.

Q7. What is the difference between the HIPAA Privacy Rule and the HIPAA Security Rule?

The Security and Privacy Rules are distinct rules but they are inextricably linked. The privacy of information depends in large part upon existence of security measures. The HIPAA Security Rule defines the standards that CEs must implement to provide basic safeguards to protect ePHI. The Privacy Rule sets the standards spelling out how CEs should may use or disclose all PHI.

In general, the Privacy Rule covers PHI in all forms (e.g., oral, written, electronic, fax, etc.) while the Security Rule only covers PHI in electronic form. The HITECH Act makes significant changes to all provisions of HIPAA of which the Privacy Rule and Security Rule are a part.

Q8. What does HIPAA mean by "ePHI" and "electronic media?"

In general, any patient medical information that has been converted to, stored in, or transmitted by electronic media is deemed to be "ePHI" and as such is to be controlled and protected under the HIPAA Privacy and Security Rules.

"Electronic media" is defined as:

- Any electronic storage media including memory in computers (hard drives)
- Any removable or transportable digital memory medium (magnetic tapes or disk, optical disk, or memory card)
- Transmission media used to exchange information electronically (Internet, leased lines, dial-up, intranets, and private networks)

The four 'operative' verbs in the HIPAA Security Rule are "create, received, maintain or transmit". When considering implementing safeguards and controls, one needs to consider all so-called information assets that create, receive, maintain or transmit ePHI and all the underlying media on which ePHI may reside?

Q9. What is the definition of an "information asset?"

"Information assets" can be thought of as the "ePHI homes". In the context of HIPAA Security, they may take the form of:

- Core networking and computing infrastructure components, services of application such as email, office applications, instant messaging, etc that comprise the "plumbing".
- Transactional systems such as billing, receivables, general accounting, payroll, patient records, etc.
- Operational systems, applications and services and/or care delivery applications such as EMR/EHR, clinical systems, departmental systems such as pharmacy, radiology applications, quality systems, etc; and,
- Strategic systems, applications and services such as data warehouses, quality and outcomes databases, informatics applications, etc.

When considering information security-related threats and vulnerabilities, it is important to consider the underlying media of each of these information assets to truly evaluate all of the "ePHI homes". For instance, the EMR application may have ePHI stored on an applications server, on a storage area network (SAN), on backup media and on end user devices.

Q10. What is the definition of "common control"?

"Common control" exists if a CE has the power, directly or indirectly, to influence or direct the actions or policies of another entity (e.g., a BA) in a significant way. This means that CEs as custodians of PHI must secure this information and take appropriate actions to ensure that outside vendors, they contracted with, also take the necessary safeguards to control and protect this PHI. As mentioned, the HITECH Act now makes the compliance, enforcement and penalties for BAs explicitly clear in that they are also completely covered by the Privacy, Security and Breach Notification regulations.

Q11. What is a "standard" as defined by the Security Rule?

A standard is a provision of the Security Rule that all CEs must comply with, specifically with respect to ePHI. There are no exceptions. There are 22 standards defined in the Security Rule. With HITECH, the number of Standards has not changed; however, more explicit guidance and clarity is provided in many areas of the Security Rule and the Privacy Rule as well. A new related rule, Breach Notification, has been promulgated by HHS as a result of The HITECH Act.

Q12. What are "implementation specifications?"

Generally, a standard defines what a CE must do while an "implementation specification" describes how it must be done. There are two types of specifications, those that are "required" and those that are "addressable." Required implementation specifications are critical and CEs and BAs, must implement them.

Addressable implementation specifications may or may not be implemented depending on the outcome of a security risk analysis and consideration of predisposing conditions and current controls the organization may have in place. For an addressable specification, a CE or BA must:

- **ASSESS** whether the specification is a reasonable and appropriate safeguard,
- **AND** implement the specification if it is reasonable and appropriate,
- **OR** document why it is not reasonable and appropriate,
- **AND** implement an equivalent alternative measure if one can be identified as reasonable and appropriate.

For years, we have been advising both CEs and BAs treat both "required" and "addressable" specifications as "required". First, it simply makes good business and risk management sense. Second, data and information is becoming more and not less vulnerable and privacy and security regulations at the federal and state level are only going to become more stringent over time.

Q13. What is a "risk analysis?"

A risk analysis is a formal process to determine and prioritize your information security exposures or risks.

The Security Rule does not specify exactly how a risk analysis should be conducted; however, the Department of Health and Human Services (DHHS) and Office for Civil Rights (OCR) issued "Guidance on Risk Analysis Requirements under the HIPAA Security Rule[1]", in July 2010. This guidance, in turn, references the National Institute of Standards and Technology (NIST) Security Framework and several specific documents such as Special Publication 800-30 Revision[2] "Revision 1 Guide for Conducting Risk Assessments – DRAFT." This NIST publication offers a comprehensive approach to completing a bona fide HIPAA Security Risk Analysis.

[1] http://abouthipaa.com/wp-content/uploads/OCR_Risk-Analysis_Final_guidance.pdf
[2] http://abouthipaa.com/wp-content/uploads/SP800-30-Rev1-ipd.pdf

A fundamental design principle in the Security Rule was that "one size does not fit all". That is, organizations needed to first understand the regulation, second assess their risks vis-à-vis the regulation and, third, take appropriate actions for their organization to mitigate their risks in order to comply with the regulation.

"Risk" is defined as the degree or likelihood that a certain threat will exploit a certain vulnerability, resulting in a compromise of safeguards designed to provide control or protection of ePHI. Risk is quantified by taking into account two factors involving (1) the likelihood of the threat exploiting the vulnerability; and (2) the impact (criticality) of loss were that threat to have exploited the vulnerability .

According to NIST SP800-30, a risk analysis is:

> *"…the process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, …, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."*

CEs and BAs must perform ongoing risk analyses in response to environmental or operational changes. A CE or BA can choose to have a third party perform the risk analysis and thus provide an independent assessment of the organization's security with respect to the HIPAA Security Standards.

Q14. What kinds of threats to security do CE's face today?

The Security Rule was designed to protect the confidentiality, integrity, and availability of ePHI. Health information that is stored on a computer, processed or transmitted across computer networks, including the Internet, is vulnerable to and must be protected from many asset/threat/vulnerability combinations including, but not limited to:

- Hacker and disgruntled employee abuse
- Untrained personnel mishandling
- Exploitation by people not having a "need to know"
- Unplanned system outages
- Burglary and theft
- Fire, flood, and other natural disasters

Q15. What safeguards does the Security Rule mandate for the protection of ePHI?

The Security Rule mandates certain technology-neutral, flexible, and scalable administrative, physical, and technical safeguards that outline which training, technologies, policies, and procedures should be put in place to ensure adequate ongoing protection of ePHI. These safeguards or controls are all based on information security best practices, many of which have been around for decades. In fact, relying on the NIST Security Framework and specifically, NIST SP800-53 Revision 3 Final, Recommended controls for Federal Information Systems and

Organizations[3], these controls are organized in families such as Administrative, Physical and Technical controls.

The original HIPAA security provisions did not mandate use of any particular technical system or safeguards. No specific guidance was provided, there was no mandate on any specific technology or approach and solutions implemented to protect ePHI were self-risk assessment based.

The HITECH Act changes this, to a degree. The Department of Health and Human Services ("HHS") must issue guidance annually on the "most effective and appropriate technical safeguards for use in carrying out" the HIPAA security standards. As mentioned above, DHHS has provided such guidance related to how to conduct a risk analysis.

Although the statute does not state that the technical safeguards set forth in HHS guidance are the only effective and appropriate technical means of satisfying HIPAA security safeguards, they are the "most effective and appropriate" means of security compliance. Those covered entities and BAs who choose not to comply with the HHS guidance should justify their choice of technical systems that are not the most effective and appropriate means of compliance.

Q16. What are some of the Technical security techniques that BAs (and CEs) may have to consider to be compliant?

The HIPAA Security Standards are largely technology-neutral. Standards in the HIPAA Security Rule are categorized into Administrative, Physical and Technical categories in sync with NIST SP800-53. As an example, the five Technical standards are: access control, audit controls, integrity, person or entity authentication, and transmission security. Again, there are a total of 22 of these standards only 5 of which fall into the Technical category.

Each standard has implementation specifications, which can be *required* or *addressable*. Remember, addressable does not mean "optional." The rule lays out the requirements and it is up to each individual organization to determine how to best meet the requirements, including which specific security technologies to implement. Now, however, on an annual basis, HHS is required to issue "…guidance on the most effective and appropriate technical safeguards". HHS is required to assess advances in information technology and security measures that CEs and BAs may use to control and protect their ePHI including:

- Firewalls
- Encryption
- Password authentication
- Digital signatures
- Secure, remote data backup
- Biometric access methods
- Anti-Spyware and Anti-virus software
- Security Auditing and Logging
- Smart cards
- Computer physician order entry (CPOE) systems

[3] http://abouthipaa.com/wp-content/uploads/10.-NIST-SP800-53-rev3-final_updated-errata_05-01-2010.pdf

Q17. When must CEs and BAs have to comply with the provisions of the Security Rule?

Most CEs were required to be in compliance with the Security Rule by April 21, 2005. However, a large portion of the Privacy Rule required certain Security Rule components to be in place as of April 14, 2003.

BAs must be fully compliant with the Security Rule by February 17, 2010. Remember, HITECH is a game-changer, especially for BAs.

- All of the HIPAA security administrative safeguards, physical safeguards, technical safeguards, and security policies, procedures, and documentation requirements apply directly to all BAs.
- HHS (and state attorneys general under the new enforcement provisions) may impose fines directly against BAs of HIPAA covered entities who do not comply with these HIPAA security standards.
- New BA security requirements must be added to all BA agreements
- All civil and criminal penalties applicable to covered entities for violating the security provisions are also applicable to BAs.

Q18. What are the consequences for non-compliance?

The original *proposed* Security Rule listed penalties ranging from $100 for violations and up to $250,000 and a 10-year jail term in the case of malicious harm. However, the final Security Rule stated that a separate regulation addressing enforcement would be issued at a later date. Therefore, under the final Security Rule:

- A penalty could be no more than $100 for each violation or $25,000 for all identical violations of the same provision
- A CE could bar the secretary's imposition of a civil money penalty by demonstrating that it did not know that it violated the HIPAA rules.
- BAs were not directly subject to liability and penalties

Here again, HITECH raises the ante literally in a very significant way. For example, a New Civil Monetary Penalty (CMP) System makes monetary penalties mandatory for violations involving "willful neglect" as of Feb. 17, 2011. Subsection 13410(c), which requires civil penalties that are collected under the HITECH Act to be funneled back into the Department of Health and Human Services' OCR enforcement budget. Section 13410(d) of the HITECH Act strengthened the enforcement by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision.

A CE and now, a BA, can no longer bar the imposition of a civil money penalty for an unknown violation unless it corrects the violation within 30 days of discovery.

The Tiered CMP System:

- Tier A is for violations in which the offender didn't realize he or she violated the Act and would have handled the matter differently if he or she had.
  - $100 fine for each violation, and
  - $25,000, maximum total imposed for the calendar year.
- Tier B is for violations due to reasonable cause, but not "willful neglect."
  - $1,000 fine for each violation, and
  - $100,000, maximum total imposed for the calendar year.
- Tier C is for violations due to willful neglect that the organization ultimately corrected.
  - $10,000 fine for each violation, and
  - $250,000, maximum total imposed for the calendar year.
- Tier D is for violations of "willful neglect" that the organization did not correct.
  - $50,000 fine for each violation, and
  - $1,500,000, maximum total imposed for the calendar year.

The new level of CMPs applies immediately to all violations. HHS will use the CMP proceeds to further enforce the HIPAA privacy and security standards and within 3 years of enactment, HHS must promulgate a regulation to distribute a portion of CMP proceeds directly to harmed individuals which will provide a direct incentive for individuals to report alleged violations to HHS and state attorneys general. It's going to get exciting!

At the same time, there are other perhaps more serious consequences for BAs than potential penalties. These include the loss of the BS's reputation and expensive lawsuits. Should a security breach occur in which ePHI is accessed by an unauthorized user, a BA could lose the trust of its customers. HIPAA's high standard could be cited in civil litigation thereby creating the potential for huge settlements.

At this writing, there are two significant cases involving BAs that are noteworthy:

- Learn from Accretive Health, Inc. Settlement with Minnesota State Attorney General[4]
- Learn from Impairment Resources bankruptcy[5]

Q19. In summary, what are the most significant changes brought about by the HITECH Act?

Before, during and after the HIPAA Security Final Rule went into effect in April 2005, there was confusion and turmoil from CEs, BAs, security professionals and government officials. It took years for people to figure out their roles and requirements under the then-new rules… and many still have not complied.

Now, with the issuance of changes under the HITECH Act, as part of American Recovery and Reinvestment Act (ARRA) of 2009, it's still surprising to hear some of the mis-statements.

- *"Our XYZ product is HIPAA compliant"*
- *"The HITECH Act doesn't change HIPAA, it just pushes electronic records."*

NOT!

[4] http://abouthipaa.com/hipaa-compliance-guides/hipaa-audit-tips-ocr-hipaa-audits-are-here-learn-from-accretive-health-inc-settlement/

[5] http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm%E2%80%99s-collapse/

- *"It doesn't apply to my small medical practice."*
- *"BAs have to comply just as they did before."*
- *"Installing the EMR doesn't change the what we do in our office."*
- *"Enforcement is only for Covered Entities; BAs just follow the contract."*

As stated above, HITECH is the largest and most consequential expansion and change to the federal privacy and security rules ever. The fifteen (15) change areas comprise new federal privacy and security provisions that will have major financial, operational and legal consequences for all hospitals, medical practices, health plans, and now their BAs and some vendors and service providers that were not previously considered BAs.

Following is a listing of key change areas brought about by the HITECH Act:

Enforcement is strengthened significantly

1. Penalties are increased in the new Civil Monetary Penalty (CMP) System
2. Enforcement is more proactive, more punitive and by more parties
3. Additional audit authority is now provided to HHS audit CEs and BAs

Business Associates and others are fully and completely "in scope"

4. BAs are now statutorily obligated to comply with the relevant regulations.
5. Adds temporary breach notification requirements to vendors of personal health records

Security Provisions are strengthened and clarified

6. Data protected is expanded beyond ePHI to include other personal information
7. More specific guidance on technical safeguards is provided by HHS annually
8. New data breach notification requirement is first-time Federal legislation on same

Privacy Provisions are strengthened and clarified

9. Individual right to request restrictions on use and disclosure of PHI is now mandatory
10. The definition of "minimum necessary" PHI to use/disclose is clarified
11. Disclosure accounting is strengthened - eliminates any exceptions from the disclosure accounting rules
12. Tightens restrictions on use of PHI for marketing purposes
13. Requires clear and conspicuous opt-out opportunity for fund-raising communications
14. Consumers now have the right to receive an *electronic* copy of their PHI
15. Prohibits a CE or BA from receiving payment in exchange for any PHI

Q20. Where can I find the complete language in the final Security Rule and HITECH Act?

The following link will take you directly to the final Security Rule in the Federal Register:

http://abouthipaa.com/wp-content/uploads/HIPAA_Security_Final_Rule.pdf

The following link will take you directly to the final ARRA Law, including the HITECH Act which is Title XIII and begins on page 112:

http://abouthipaa.com/wp-content/uploads/Full_ARRA_Law_incl_HITECH_Act.pdf

Q21. In practical terms, what should I do first?

Whether you are a CE or a BA, following is a short checklist of critically important actions you should take as soon as possible:

A. Set Privacy and Security Risk Management & Governance Program in place (45 CFR § 164.308(a)(1))
B. Complete a HIPAA Security Evaluation (= compliance assessment) (45 CFR § 164.308(a)(8))
C. Complete a Privacy Rule compliance assessment (45 CFR §164.530)
D. Complete a Breach Rule compliance assessment (45 CFR §164.400)
E. Complete a HIPAA Security Risk Analysis (45 CFR §164.308(a)(1)(ii)(A))
F. Develop comprehensive HIPAA Privacy and Security and Breach Notification Policies & Procedures (45 CFR §164.530 and 45 CFR §164.316)
G. Document and act upon a remediation plan

Q22. How can Clearwater Compliance help?

Clearwater Compliance LLC (http://ClearwaterCompliance.com) assists CEs and BAs throughout the U.S. with all matters related to compliance with the HIPAA Privacy and Security Rule standards and the new HITECH provisions.

To assist our customers with the burdensome impact of the HIPAA Security Rule and the HITECH Act security and privacy provisions, we have developed and offer:

1. Compliance tools and software;
2. Professional services and consulting; and,
3. Remediation solutions

For more information or to schedule a HIPAA-HITECH Security compliance assessment at your offices, please contact us on **(800) 704-3394**.