HIPAA / HITECH Compliance Risks with Visual Basic 6.0

Robert Encarnacao & Erick Nassar

May 2011

Table of Contents

Introduction: the HIPAA and HITECH regulations

The Health Insurance Portability and Accountability Act[1] (HIPAA) is a public law enacted by the US Congress in 1996. It has four main objectives. These include the improvement of portability and continuity of health insurance coverage. Additionally, it aims to avoid waste, fraud and abuse in health insurance and healthcare delivery. A third goal is the reduction of costs and administrative burdens of healthcare by improving the efficiency and effectiveness of the system through the standardization of the interchange of electronic data for specified administrative and financial transactions. And lastly, it aims to protect the privacy of records by ensuring the security and confidentiality of healthcare information. So, HIPAA basically aims to:

- Improve portability and continuity of coverage
- Avoid waste, fraud and abuse
- Reduce costs and administrative burdens
- Protect the privacy of records

The legislation carries grave civil and criminal penalties for failure to comply. Civil penalties include fines that range from $100 per violation to $250,000 per calendar year, and the US Department of Justice will enforce criminal penalties which may include up to 10 years imprisonment and a $250,000 fine[2].

The Health Information Technology for Economic and Clinical Health Act[3] (HITECH), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA), widens the scope of privacy and security protections available under HIPAA. In turn, it increases potential legal liability for non-compliance and provides more enforcement of HIPAA rules. ARRA contains incentives related to healthcare information technology, in general, - some specifically designed to accelerate the adoption of electronic health record (EHR) systems among providers. For example, civil penalties for willful neglect are increased under the HITECH Act, extending up to $1.5 million for repeat/uncorrected violations, plus certain HIPAA security provisions directly apply now to business associates, such as software vendors providing EHR systems. The HITECH Act has focused on the establishment of a national health infrastructure and on ensuring improved privacy protections, placing both HIPAA's Privacy Rule and Security Rule as critical challenge for healthcare providers.

---

[1] United States Government Printing Office. *Health Insurance Portability and Accountability Act of 1996.* http://www.gpo.gov/fdsys/pkg/CRPT-104hrpt736/pdf/CRPT-104hrpt736.pdf

[2] American Medical Association. *HIPAA Violations and Enforcement.* http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page

[3] United States Government Printing Office. *American Recovery and Reinvestment Act of 2009*. http://www.securityprivacyandthelaw.com/uploads/file/ARRA.pdf (title XIII, page 112)

HIPAA's provisions and Information Systems

HIPAA is comprised of five Titles. Title I guarantees access, renewal and portability of health insurance. Title II addresses cost reduction, administrative simplification, and fraud and abuse. Title III establishes medical savings accounts. Title IV sets group plan regulations; and Title V encompasses revenue offsets.

The provisions with the greatest impact to Healthcare Organizations are those contained in Title II, which call for the development of national standards to protect the privacy of Americans' healthcare records. This title, known as the Administrative Simplification provision, requires the establishment of national standards for electronic healthcare transactions and national identifiers for providers, health insurance plans, and employers. It constitutes a method of making business practice uniform in the areas of billing, claims, computer systems and communication so that providers and payers do not have to change the way in which they interact with each other through each other's proprietary systems. That includes activities such as enrolling an individual in a health plan, paying insurance premiums, checking eligibility, obtaining authorization to refer a patient to a specialist, processing claims or notifying a provider about the payment of a claim. This will reduce costs and improve efficiency through the implementation of a standardized electronic data interchange. In turn, these savings would be available to toward improving of healthcare quality and availability. In fact, the net savings over 10 years were estimated at $12.3 billion[4]. However, this title also includes a series of regulations oriented towards guaranteeing the privacy and security of the critically sensitive data involved in these systems.

In healthcare today, reliable information about individuals is critical to providing high quality coordinated care. Data corruption or inaccuracy can have life-threatening consequences. As well, numerous forces have been driving the healthcare industry towards advances in the use of health information technology, such as the potential for reducing medical errors and healthcare costs, and increasing the patients' involvement in their own health care.

HIPAA created specific requirements for managing health information privacy and security, dramatically changing the legal and regulatory environment for managing patient medical data. One of these mandates is to protect health information by establishing transaction standards in security and privacy for the exchange of health information.

[4] Grimes, Stephen. *Is Your Security Back Door Open? HIPAA's Implications for Biomedical Devices & Systems.* HIMSS, USA, 2002. http://www.himss.org/content/files/proceedings/2003/Sessions/session64_slides.pdf (slide #14).

HIPAA: The Security Rule

There are a series of regulations, called the “Security Rule”, which specify administrative, physical, and technical safeguards for covered entities, establishing standards for all health plans, clearinghouses and storage of healthcare information to properly ensure the confidentially, integrity and availability of electronic protected health information:

- Confidentiality assures that data is shared only among authorized persons or organizations.
- Integrity assures that data is accurate, authentic and complete, and that cannot be changed unless an alteration is known, required, documented, validated and authoritatively approved.
- Availability assures that systems responsible for delivering, storing and processing critical data are accessible when needed, by those who need them, under both routine and emergency circumstances.

These standards apply to healthcare providers, insurance plans, and data clearinghouses:

Covered Entities: Who needs to comply with the Security Rule?		
HEALTHCARE PROVIDERS	**HEALTH INSURANCE PLANS**	**HEALTHCARE CLEARINGHOUSES**
• General practitioners • Specialists • Hospitals and clinics • Diagnostic, laboratories and imaging centers • Pharmacies • Nursing Homes • Ambulance Services • Dental Services • Mental Health Services • Physical therapy and other outpatient services	• Major medical / traditional fee-for-service plans • Managed care plans: HMO. PPO, POS, EPO • Consumer or self-directed plans • Self-funded corporate plans • Government programs: Medicare, Medicaid, and the Veterans Health Administration	Entities that process standard and non-standard health information they receive from other entities into standard electronic formats for purposes of processing insurance claims, patient billing or the storage of patient data.

HIPAA: The Privacy Rule

HIPAA also includes a "Privacy Rule", which establishes the national standards as to who may have access to Electronic Patient Health Information (ePHI). The rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization[5].

While the Privacy Rule sets the standards for ensuring that only those who should have access to this data will actually have access, it is the requirements of the Security Rule which have the largest impact on healthcare organizations in terms of both technical and organizational compliance challenges. Basically, the HIPAA Security Rule makes sure the ePHI is not disclosed improperly, and that hackers can't easily gain access to Electronic Medical Records (EMRs). Protection of data from unauthorized access, whether external or internal, stored or in transit, is all part of the Security Rule[6].

To accomplish this, each covered entity is required to meet 3 basic conditions[7]:

1. Assess potential risks and vulnerabilities to the individual health data in its possession.
2. Develop, implement, and maintain appropriate security measures, which must include, at a minimum, the following requirements and implementation features:
    a. Administrative Procedures
    b. Physical Safeguards
    c. Technical Security Services and Mechanisms
3. Ensure these measures are documented and kept current.

Data covered by this rule, for example, may reside in the following servers, workstations, networks, terminals, peripherals, web sites, application service providers and claims processing systems.

Implementing the necessary safeguards required by HIPAA implies the requirement for more sophisticated technologies than was has traditionally been available in the 1990's. The security standards do not dictate or stipulate the use of specific technologies, but legacy software will insure increased risk of systems compromises. With the

---

[5] U.S. Department of Health and Human Services. *Health Information Privacy: The Privacy Rule.* http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html
[6] U.S. Department of Health & Human Services. *Health Information Privacy: The Security Rule.* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html
[7] U.S. Department of Health & Human Services. *Guidance on Risk Analysis Requirements under the HIPAA Security Rule.* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

prospect of severe civil and criminal penalties from the Department of Justice or a state's Attorney General's office even for minor infractions, it is critically important to take the necessary precautions and ensure full compliance.

Appropriate technical safeguards include:

1. Ensuring that applications are built using the latest technologies which incorporate advances in security features and best-practices.
2. Mitigating the risk of breaches that make critical data vulnerable.
3. Making sure that all software running on the systems is currently supported by the vendor as this guarantees access to updates and patches providing an added layer of security.

Protected Health Information

Protected Health Information, also referred to as "PHI", can be breached in any of the commonly recognized data states as shown below in the diagram 1, below. Data is considered "in motion" while it is moving through networks, over wireless transmissions such as communications with a clearinghouse or an email or by means of fax. Data is considered "at rest" when it is residing in a file system, database or any other structured form of storage. It can all be "in use" when it is being updated, created or reviewed. Likewise, it's "disposed" state, whether electronic or paper records, is also a state in which the PHI should be unusable, unreadable or indecipherable to unauthorized individuals, with the minor exception that PHI is no longer "protected" once it has been "deidentified". [8]

PHI is rendered unusable, unreadable or indecipherable to unauthorized individuals and thus in compliance if one or more of the following applies:

1. Electronic PHI when in motion and at rest must be encrypted as specified in the HIPAA Security Rule and that the encryption key has not been breached. While at rest, valid encryption processes include those consistent with the National Institute of Standards and Technology, NIST, Special Publication 800-11, *Guide to Storage Encryption Technologies for End Use Devices*[9]. And while in motion, data must comply with different set of

[8] Department of Health and Human Services. *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII of the American Recovery and Reinvestment Act of 2009.* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechrfi.pdf
[9] National Institute of Standards and Technology. *Guide to Storage Encryption Technologies for End User Devices.* *http://static.hipaa.com/documents/SP800-111.pdf*

standards such as Transport Layer Security (TLS) and Virtual Private Networks (VPNs) such as Internet Protocol Security (IPsec) and Secure Socket Layer (SSL).

2. For electronic media in the disposed state it must have been cleared, purged or destroyed consistent with NIST's *Guidelines for Media Sanitation* such that the PHI cannot be retrieved. Media sanitation is further divided into four categories: disposal, clearing, purging and destroying. [10]

Technical safeguards include access, audit and integrity controls in addition to transmission security. Technical policies and procedures that allow only authorized personnel to access electronic PHI must be implemented. Hardware, software and other mechanisms to record and monitor access and other activity in the systems that come in contact with electronic PHI need to be created. Electronic measures must be put into place to ensure that this information is not improperly altered or destroyed. And finally, there needs to be a means to guard against unauthorized access to electronic PHI while it is in transmission over an electronic network.

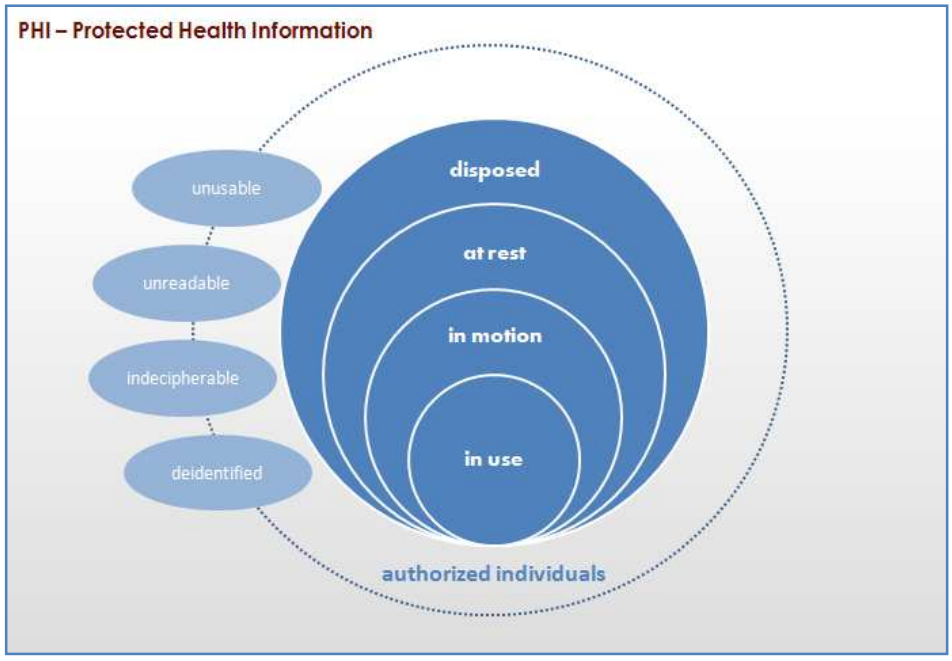

DIAGRAM 1 *– Visualization of the protected health information (PHI) states.*

[10] National Institute of Standards and Technology. *Guidelines for Media Sanitation.* http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Microsoft's Visual Basic 6 and the .NET platform

Over the past 10 years, each release of the .NET platform and its corresponding programming languages and development environments has had a particular theme that was marketed louder than others, e.g., managed code, generics, Language Integrated Query (LINQ), Dynamic Language Runtime (DLR), there have been other countless improvements in C# and VB.NET over the legacy platform, Visual Basic 6, each offering to remedy previous shortcomings and providing advances in security features and best-practices.

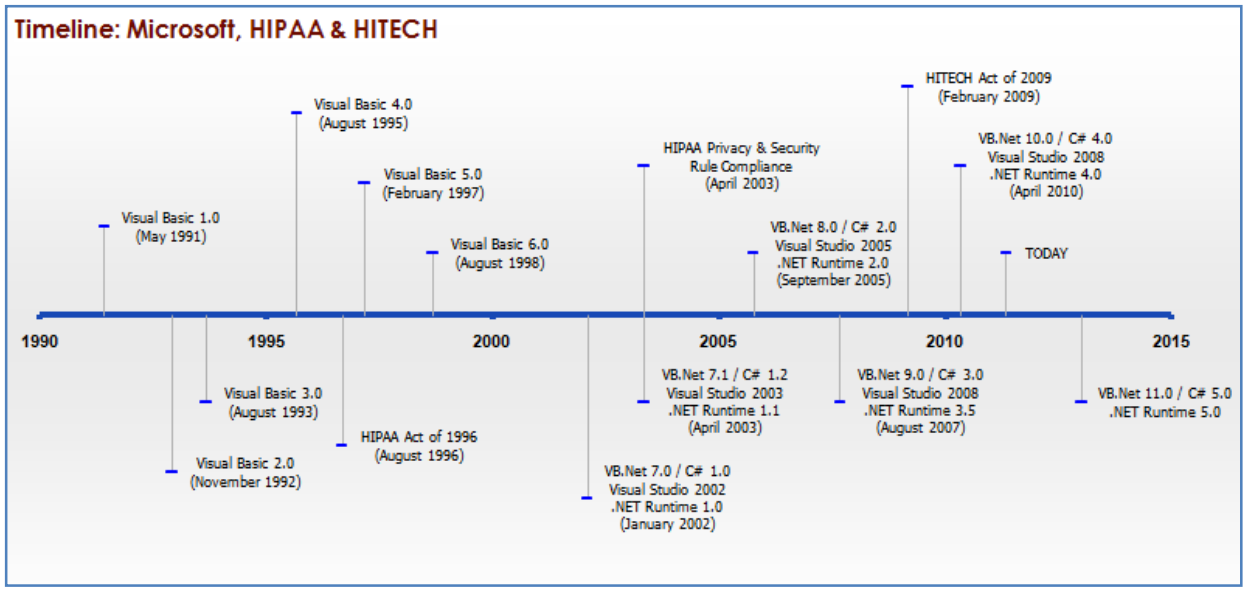

DIAGRAM 2 *– Overlapped Microsoft, HIPAA and HITECH milestones from 1990 to 2015.*

The new development environments offer better modeling of business objects with increased support for design patterns and efficient architectural options. With .NET, the introduction of the "try/catch" syntax in Visual Basic allows for improved error handling techniques over the previous "On Error" approach. Strict type checking and tighter control on variable scope and member permeability offer modern data typing disciplines and simpler data validation. Long gone are the days of the "variant" – often an entry point for hackers and a source of performance limitations with large memory overheads. New support for the Long datatype will reduce the messy hacks previously used to support 64-bit numerical operations. The elimination of versioning problems typically associated with "DLL hell", the inability to create Windows services and dependencies on fragile COM Registry entries are no longer an issue with the .NET Framework. Functionally-equivalent code written in .NET simply requires less code. Less code generally translates to fewer bugs and entry points for potential hackers. Additionally, these .NET languages provide for true support for multithreading and 64-bit application development. More than just allowing for true object-oriented programming, .NET programming languages offer a wider degree of options for language paradigms. All of this amounts to serious improvements over Visual Basic 6.

The last release of Visual Basic 6 arrived in 1998 and its mainstream support ended in March of 2005. Microsoft even ended its extended support in March 2008. Visual Basic 6 is quickly approaching its 15th birthday and is clearly no longer the latest technology. Real-world advances in security and improvements in application development best-practices are no longer available to Visual Basic 6 applications. Without access to updates and patches, it's no longer feasible to mitigate the risk of vulnerability to security breaches of critical data.

While Visual Basic 6 will indeed hobble on in Windows 7 environments until about 2020 according to Microsoft[11], it will most likely go no further. The ability for software developers to respond to serious lingering issues and new threats on the unsupported platform continues to wane. Continuing down the road of VB6 obsolescence creates a real security risk in terms of human resources. In addition to all the benefits mentioned above, a modernized application creates an environment that helps to sustain high job satisfaction and ultimately greater retention, - both ingredients vital to HIPAA compliance as they lower the risk of negligent data handling and theft. Making the jump to the .NET platform, whether VB.NET or C#, is a low risk strategy for healthcare providers, insurance plans and clearinghouses, despite what might seem like the daunting task of migration. Such a move, however, will establish a technology foundation capable of meeting current and future needs especially in the face of rules that are expected to change often.

Preserving VB6 Applications

As desktops continue to be updated to the last operating system versions or service packs, it is clear that eventually the older Visual Basic 6 applications will cease to function. But before the application quits working altogether, there will be noticeable consequences of preserving the legacy application.

Consequences of preserving your VB6 application on Windows 7 include:

- User Interface Issues
- Decreased Functionality
- Broad Security Risks
- Performance Latency
- Lack of Technical Support
- Forward Incompatibility

[11] Microsoft Visual Basic Development Center. *Support Statement for Visual Basic 6.0 on Windows Visa, Windows Server 2008 and Windows 7.* http://msdn.microsoft.com/en-us/vbasic/ms788708.aspx

Many of the more common place consequences will include user-interface issues. Many user controls previously compatible with Windows XP and other version, will no longer be compatible with Windows 7. There are also Windows API calls that have are no longer available. Similarly, the “SendKeys” functionality is no longer supported. The lack of technical support is a bit issue. The Visual Basic 6 development environment doesn’t run on Windows 7 without the use of a virtual machine. There has been no support available for the development environment since April 8, 2008. With lots of potential security risks, these applications often have to “run as administrator”. Business operations may require integration between this older application with new applications; such integrations may prove unfeasible or very costly.

Even Microsoft recognized the near-futility of running a VB6 application on Windows 7 by providing a free virtual PC for Enterprise and Ultimate editions of the operating system. While this may offer some relief, many applications experience performance latency and hanging.

Managed Code

Beyond VB6, managed code reduces vulnerabilities that are inherent to programmers, such as having to handle their own memory management. Managed code also reduces risks of unintentionally opening up security holes that are inherent in low-level system interactions. The .NET Framework offers better coding models to this end. For instance, the Common Language Runtime (CLR) provides file format and metadata validation. Microsoft Intermediate Language (MSIL) code verification ensures type safety, prevents bad pointer manipulations and virtually eliminates buffer overflow vulnerabilities. The integrity of “strong-named” assemblies, in lieu of traditional GUIDs, is verified using a digital signature that ensures that the assembly was altered in any way since it was built and “signed”. This means that attackers cannot alter your code in anyway by directly manipulating the MSIL instructions. From a security perspective, .NET managed code offers significant improvements over Visual Basic 6. [12]

[12] http://msdn.microsoft.com/en-us/library/cwk974ks%28vs.71%29.aspx, http://msdn.microsoft.com/en-us/library/ff648652.aspx

User and Code Security

Both role-based and code-access security are layered on top of Windows security in the .NET Framework. While role-based security controls user access to application-managed resources, code-access security is concerned with which code can access which resources and perform which privileged operations. For Web application, this is an enormously beneficial security feature because it restricts what a likely attacker is able to do if it managed to compromise the Web application process. This feature also provides application isolation – particularly important for hosting companies. The two security features offer a great advantage of traditional Visual Basic applications.

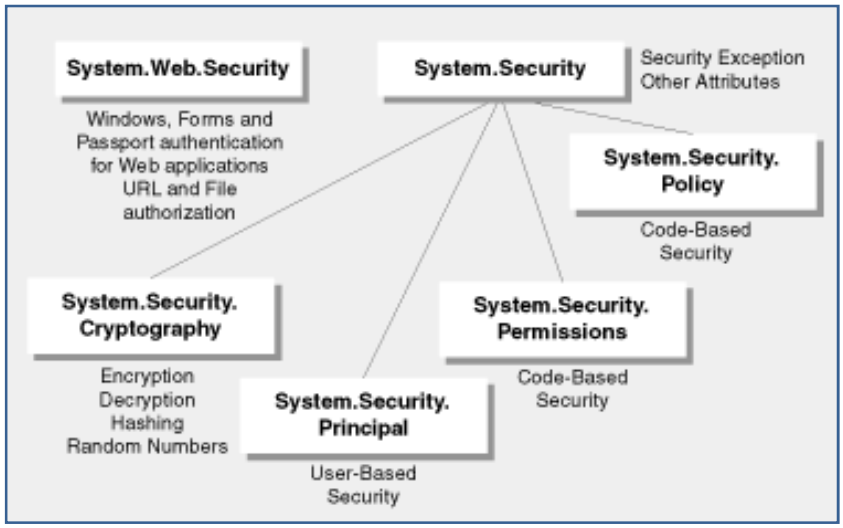

DIAGRAM 3 *– Microsoft .NET security namespaces.*

Conclusions

With HITECH widening the scope of compliance concerns for HIPAA's Privacy and Security Rules, participants in the health care industry, including providers, insurance companies, clearinghouses and software vendors, not just the corporate entities but employees and business associates as well, should be aware of the possible enforcements measures that could be taken upon them if standards aren't met. Compliance issues can now result in felony prosecutions of up to 10 years in prison as well as millions of dollars in civil penalties. The security provisions of these laws apply directly to software vendors who provide the systems to the industry and those that administer the systems. They will now be held legally accountable for the confidentiality, integrity and availability of their patient data.

While HIPAA and HITECH do not call for the use of any specific software, it does suggests using software that has vendor support and access to updates and patches that will reduce the risk of non-compliance. So the VB6 IDE, which Microsoft stopped supporting years ago, could represent a violation, even though the runtime is still OK. Moreover, even if a legacy VB6 application is able to run on Windows 7, it is likely to encounter issues – many of which may compromise security, availability or functionality. Upgrading to .NET makes it easier to implement technology to stay in compliance with other areas of HIPAA/HITECH, like keeping the data secure in transmission and encryption. Regardless, not having a compliance plan in place will be considered "willful neglect" by enforcement authorities.

Software companies and their developers can no longer afford to treat security as an afterthought. They must ensure that applications being built and supported are using the latest technologies, – incorporating recent advances in security features and best-practices. Penalties are now being imposed[13] as attorneys general offices nationwide are seeking the every widening options and availability for HIPAA enforcement training.[14] Fortunately, Microsoft has placed security-related features at the core of the .NET Framework and forces developers regardless of carelessness or lack of experience to address security both from use of managed code, role-based and code-access security and the rich libraries in the .NET security namespaces. The necessary next step for many organizations is to migrate their Visual Basic 6 legacy application to .NET to remove completely the risk of VB6 obsolescence.

[13] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html
[14] http://www.workplaceprivacyreport.com/tags/hipaa-enforcement-training/