HIPAA Secure Now!

How MSPs Can Profit From Selling HIPAA security services

HIPAA Secure Now!

How MSPs can profit from selling HIPAA security services

Managed Service Providers (MSP) can use the Health Insurance Portability and Accountability (HIPAA) security services to grow their business. This paper will give valuable insight into how HIPAA security services can help MSPs enter or expand their services into the rapidly growing healthcare information technology (HIT) market. The HIT market is one of the fastest growth areas in the economy driven by the government's Meaningful Use incentive program which provides physicians up to $44,000 if they implement electronic health records (EHR). MSPs can leverage the fact that covered entities (healthcare organizations, physician, dental and chiropractic practices) are required to perform a HIPAA risk assessment. A HIPAA risk assessment identifies areas where additional security is required to protect patient information; it can therefore justify the need for additional services such as offsite backup, disaster recovery, encryption, etc. Finally we will go over the HIPAA Secure Now! partner program and show how MSPs can leverage our services to take advantage of the opportunities that HIPAA provides to MSPs.

Rapid Growth of Healthcare Information Technology

In February 2009, the American Recovery and Reinvestment Act ("the Stimulus Bill") was signed into law by the Federal Government. This new law set aside $27 billion under the Health information Technology for Economic and Clinical Health Act (HITECH Act) to foster increased use of Electronic Health Records (EHRs) by physicians and hospitals. The incentive program also known as "Meaningful Use" provided covered entities (healthcare organizations, physician, dental and chiropractic practices) with additional Medicare payments if they implemented EHRs. A physician could qualify for up to $44,000 of additional payments over 5 years under the Meaningful Use program.

Medicare EHR Incentive Payment Schedule

Year of adoption	Incentive payout over time			
Payment Amount for 2011	$18,000			
Payment Amount for 2012	$12,000	$18,000		
Payment Amount for 2013	$8,000	$12,000	$15,000	
Payment Amount for 2014	$4,000	$8,000	$12,000	$12,000
Payment Amount for 2015	$2,000	$4,000	$8,000	$8,000
Payment Amount for 2016		$2,000	$4,000	$4,000
Total Payment Amount	**$44,000**	**$44,000**	**$39,000**	**$24,000**

The success of the Meaningful Use program is driving the use of EHRs. According to The U.S. Centers for Medicare and Medicaid Services (CMS), approximately 80% of eligible hospitals and 50% of eligible physicians have adopted EHRs and received incentive payments from Medicare and Medicaid. These providers received more than a combined $4.2 billion in just over two years of the program.

Healthcare Information Technology Impact

As a result of the push to implement EHRs and associated Health Information Technology (HIT), the HIT market is one of the fastest growing markets in the United States. The HIT market was valued at $40.4 billion in 2012 and will grow to $56.7 billion by 2017 according to analysts.

Patient Record Breaches on the Rise

As the push to implement EHRs grows so does the amount of patient records breached. According to the United States Department of Health and Human Services (HHS), more than 20 million patient records have been breached since 2009. Numerous breaches resulted from lost or stolen laptops, smartphones, tablets, USB drives and other portable media. Insecure emails and stolen records due to hackers and dishonest or careless employees are also drivers of breach incidents.

Increased HIPAA Enforcement

In response to this epidemic of patient record breaches, the HHS Office of Civil Rights (OCR), which is tasked with enforcing the HIPAA regulations, has committed to ensuring that HIPAA regulations are strictly enforced and patient information is protected. OCR implemented a pilot program in 2012 that randomly audited 115 healthcare organizations of all sizes. The audits included billion dollar healthcare corporations, insurance companies, and even small physician practices. OCR is evaluating the pilot audit program and is committed to implementing a permanent HIPAA audit program in late 2013 or early 2014.

HHS has recently announced the HIPAA Final Omnibus Rule. The Omnibus Rule expands HIPAA regulations to HIPAA business associates, increases penalties for non-compliance and puts more burden on organizations that have patient record breaches. According to the HHS Press Release:

> "The final omnibus rule greatly enhances a patient's privacy protections, provides individuals new rights to their health information, and strengthens the government's ability to enforce the law.
>
> The changes announced today expand many of the requirements to business associates of these entities that receive protected health information, such as contractors and subcontractors. Some of the largest breaches reported to HHS have involved business associates. Penalties are increased for noncompliance based on the level of negligence with a maximum penalty of $1.5 million per violation. The changes also strengthen the Health Information Technology for Economic and Clinical Health (HITECH) Breach Notification requirements by clarifying when breaches of unsecured health information must be reported to HHS."

HIPAA Risk Assessment is a Core Requirement

The HIPAA Security Rule requires organizations to protect the confidentiality, integrity and availability of electronic protected health information (ePHI or patient information). Organizations are required to implement effective and appropriate administrative, physical, and technical safeguards to protect patient information. A core requirement of the HIPAA Security Rule specifies that an organization conduct a HIPAA Risk Assessment / Risk Analysis on how it is currently protecting patient information and implement additional safeguards to further protect patient information. According to HHS:

> "All ePHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process."

Meaningful Use Requirement

A HIPAA security risk assessment is also a core requirement under the Meaningful Use requirements. In order to receive payments, the risk assessment must be done on an annual basis. According to HHS Health Resources and Services Administration (HRSA):

> "To receive the incentive payments, you must also demonstrate that you have met the criteria for the EHR Incentive Program's privacy and security objective. This objective, "ensure adequate privacy and security protections for personal health information," is the fifth and final health policy priority of the EHR Incentive Program. The measure for Stage 1 aligns with HIPAA's administrative safeguard to conduct a security risk assessment and correct any identified deficiencies. In fact, the EHR Incentive Program's only privacy and security measure for Stage 1 is to:
>
> > *Conduct or review a security risk assessment of the certified EHR technology, and correct identified security deficiencies and provide security updates as part of an ongoing risk management process.*
>
> The risk analysis and risk management process must be conducted at least once prior to the beginning of the EHR reporting period. You will need to attest to CMS or your State that you have conducted this analysis and have taken any corrective action that needs to take place in order to eliminate the security deficiency or deficiencies identified in the risk analysis."

The output of a comprehensive HIPAA Risk Assessment includes recommendations that an organization should implement to increase the security of patient information. By performing a HIPAA Risk Assessment, an organization is forced to identify where patient data is stored or transmitted, specify how it is being protected and examine the threats or vulnerabilities to that data

A thorough HIPAA Risk Assessment can identify threats to patient data that could cause security breaches. Implementing the recommendations of a HIPAA Risk Assessment could significantly lower the risk of HIPAA breaches and the potential of penalties for non-compliance with HIPAA regulations.

Common Findings of a HIPAA Risk Assessment

Some of the common findings of a HIPAA Risk Assessment include the following:

- Lack of encrypted offsite data backup
- Lack of an implemented and tested disaster recovery plan
- Lack of email encryption
- Lack of laptop encryption
- Lack of mobile encryption (smartphones / tablets / USB drives, etc.)
- Lack of anti-virus on all endpoints and servers
- Lack of security patching of servers and desktops
- Lack of security penetration and vulnerability testing
- Lack of security incident response procedures

A HIPAA Risk Assessment would determine risks of threats to ePHI and recommend that appropriate security safeguards be implemented to address the above findings and lower the risk to ePHI.

MSPs Can Help Implement the Risk Assessment Recommendations

A HIPAA Risk Assessment can help sell many of the services that MSPs offer. Many of the common findings of a HIPAA Risk Assessment can be addressed by products and services available from the MSPs. Typical MSPs core functions include data backup, disaster recovery, anti-virus services and security patching of servers and desktops. MSPs can also play a valuable role in helping organizations with implementing encryption services.

A MSP can also help implement a security incident response plan. A MSP can play a core role in reacting and responding to security incidents including a lost or stolen laptop or smartphone, a hacker breaching an organization's infrastructure or a virus infiltrating an organization's network.

HIPAA Secure Now!

HIPAA Secure Now! has helped healthcare organizations since 2009 to comply with the HIPAA Security Rule and protect patient information. HIPAA Secure Now! provides the following services to clients:

- Perform a thorough HIPAA Risk Assessment
- Write HIPAA security policies and procedures
- Train employees on HIPAA security
- Provide security breach response steps and documentation
- Help track business associates

- Provide ongoing advice and guidance on HIPAA security

HIPAA Secure Now! plays a critical role in helping organizations comply with HIPAA requirements and protect patient information. HIPAA Secure Now! are experts in the HIPAA Security and Omnibus Rules. The streamlined HIPAA Risk Assessment process provides valuable insight into the areas where organizations need to increase their security safeguards while minimizing a client's time spent on performing the Risk Assessment. The HIPAA policies and procedures are written for the client organization and made available to employees along with engaging videos that explain each policy. The online employee security training and compliance testing has been very well received as being very insightful as well as interesting and engaging. Employees actually enjoy taking the HIPAA Secure Now! employee security training. Finally, HIPAA Secure Now! is priced to be affordable by organizations of every size.

HIPAA Secure Now! Partner Program

HIPAA Secure Now! (HSN) has built a partner program that is a perfect complement to the services already offered by for MSPs. HSN provides the expertise in the HIPAA security requirements which allows MSPs to leverage the benefits of HIPAA without being experts themselves. The HSN partner program can enable MSPs to enter or expand their services into the rapidly growing Healthcare Information Technology market.

Strong Partnership

The HSN partner program is built around a strong partnership between HSN and our partners. We want to provide our partners with the tools and resources to engage clients in HIPAA security services. We understand the importance of the relationship between our partners and their clients / customers. HSN is committed to helping our partners succeed and we vow never to come between our partner and their clients. Our partnership philosophy is embodied in the following statement:

> ***"We can complement and supplement the services you already offer, but we will never compete with them"***

Reseller Options

The HSN partner program provides a healthy margin to MSPs. MSPs can expand their service offerings to include HIPAA security services and thereby increase their bottom-line. MSPs receive a referral commission on the initial sale to a client as well as recurring commissions on subsequent annual compliance subscription sales. An MSP will receive referral commissions as long as the client subscribes to the annual compliance subscription.

We offer flexible ways to resell the HIPAA Secure Now! service. Some partners want to own the billing process with their clients and others simply want to refer clients to HIPAA Secure Now! The HSN partner program supports both methods of reselling the HIPAA Secure Now! service. Partners can refer clients

to HIPAA Secure Now! and receive a referral commission payment on the sale. Partners can also purchase the HIPAA Secure Now! service at a discount, equivalent to their referral commission, and bill the client directly for the HIPAA Secure Now! services. Some HSN partners add value to the HIPAA Secure Now! service and charge clients a premium on the service to reflect the value. The HSN partner program's flexibility allow for various ways to resell the service.

Bundling HSN into MSP Services

Some of the HIPAA Secure Now! MSP partners elect to bundle the HSN services into their MSP service offerings. Some of the HSN MSP partners have created a HIPAA compliance service offering that includes the HSN service along with the core MSP product offering. Bundling the HSN services allows an MSP to market and differentiate themselves from other MSPs and competitors. In addition to the ability to market a bundled HSN offering to HIPAA covered entities, the bundled HSN service allows MSPs to take advantage of the project opportunities which arise from a client performing an annual HIPAA Risk Assessment.

Benefits of a HIPAA Risk Assessment

HSN partners can benefit from clients performing a HIPAA Risk Assessment. A HIPAA Risk Assessment can help sell additional MSP services. For instance, a HIPAA Risk Assessment might identify the need for a client to implement disaster recovery, security patching or other services that MSPs can offer. MSPs can use the HIPAA Risk Assessment to engage clients in a thorough evaluation of their network security. MSPs can become a trusted partner helping a client implement the required security measures to comply with HIPAA regulations and lower the risk to patient information.

Next Steps

The HIPAA Secure Now! partner program can help MSPs expand their service offerings to include HIPAA security services. The healthcare information technology (HIT) market is one of the fastest growing segments of the economy. Millions of HIPAA covered entities are required to comply with HIPAA requirements. The HSN partner program allows MSPs to differentiate themselves and market directly to HIPAA covered entities. The flexibility of the HSN partner program enables MSPs to protect their relationship with clients / customers while providing various ways of engaging a client in HIPAA security services. MSPs can leverage a client's HIPAA Risk Assessment to sell additional services, while helping clients with HIPAA compliance and lowering the risk to patient information.

To request more information or to discuss the HSN partner program in-depth, please visit our HSN Partner Page at http://www.hipaasecurenow.com/index.php/partners/