HITECH, HIPAA, Rewards, Risks

Important Facts Small and Mid-size Healthcare Organizations Need To Know To Reap HITECH Rewards and Avoid HIPAA Risks

NetGain TECHNOLOGIES

Overview

This NetGain Technologies white paper highlights key provisions of the recently finalized Health Information Technology for Economic and Clinical Health (HITECH) Act. In addition, it offers specific examples of how small and mid-size healthcare providers are using health information technology (HIT) and electronic health records (EHR) to improve patient care and lower operating costs.

This white paper also discusses: (1) The revised – and substantially higher – penalties that can now be levied (with examples of recent regulatory actions) against any covered entity found in violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy rules and (2) What to look for in a solutions provider to ensure success with both HIT implementation and HIPAA compliance.

Rewards

"An unprecedented federal effort is underway to boost the adoption of electronic health records and spur innovation in health care delivery....We found that 92 percent of the recent articles on health information technology reached conclusions that were positive overall. We also found that the benefits of the technology are beginning to emerge in smaller practices and organizations, as well as in large organizations that were early adopters."[1]

We found that 92 percent of the recent articles on health information technology reached conclusions that were positive overall. We also found that the benefits of the technology are beginning to emerge in smaller practices and organizations....

The above quote is from *Health Affairs*, a leading health policy thought and research journal. The "unprecedented federal effort" it refers to is being spurred in large part by the HITECH Act, itself a major component of the American Recovery and Reinvestment Act signed into law in February 2009. A key provision of the HITECH Act makes as much as $27 billion in incentive payments available to healthcare providers for the adoption and meaningful use of technology that enables electronic health records (EHR).[2]

As for specific details on these federal incentive payments we offer the below summary, taken from the *Centers For Medicare & Medicaid Services* web site:

> "The Medicare and Medicaid EHR Incentive Programs provide incentive payments to eligible professionals, eligible hospitals and critical access hospitals as they adopt, implement, upgrade or demonstrate meaningful use of certified EHR technology. Eligible professionals can receive up to $44,000 through the Medicare EHR Incentive Program and up to $63,750 through the Medicaid EHR Incentive Program."

As of February 2013, more than 234,000 healthcare providers had received payments from the program.[3] Information on how to qualify for the HITECH Act incentives can be found at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html.

Of course, the biggest rewards from the HITECH Act won't come from reimbursement payments but in the improved patient care capabilities and ongoing cost-savings that HIT/EHR enables. While the transition to EHR is still in its infancy (especially for smaller practices and caregiver organizations) and not without significant challenges, the benefits of EHR implementation have been clearly established.

Patient care benefits

Patient care benefits of EHR are numerous. According to HealthIT.gov, an HHS website, these benefits include:

- **Improved care coordination** – Of those providers using fully functional EHR:
  - — 72% reported that EHR positively affected communication with patients.[4]
  - — 74% reported using an EHR system resulted in enhanced overall patient care.[5]
- **Enhancement of provider's capabilities to care for patients** – HealthIT.gov cites two separate studies showing (1) A higher standard of patient care by EHR-enabled medical practices and (2) Annual improvements in care by EHR-enabled practices that were 10% greater than those of paper-based practices.[6]

Financial benefits of EHR implementation

As with all IT investments, it's important that any outlay for HIT show a meaningful economic return. Properly deployed, with expert help and adequate training, there's every reason to expect that your HIT investment *will* pay off.

- According to a 2005 article published in *Health Affairs*, case studies of fourteen solo or small-group primary care practices found that the average practice paid for its EHR costs in 2.5 years and profited handsomely after that.[7]
- A 2007 peer-reviewed article published in the *Journal of the American College of Surgeons* studied the impact of EHR implementation at an academic medical center with 5 offices and 28 providers. The study showed that EHR implementation resulted in an annual savings of $393,662. And, that the medical center recouped its original investment within 16 months.[8]
- Within one year of implementing an EHR system, Staten Island, New York sole practitioner (internal medicine) Salvatore Volpe, MD, had recouped his full investment and was earning over $30,000 more than he had the

Within one year of implementing an EHR system, Staten Island, New York sole practitioner (internal medicine) Salvatore Volpe, MD, had recouped his full investment and was earning over $30,000 more than he had the year before, due primarily to reduced overhead costs.

year before, due primarily to reduced overhead costs.[9]

- Palm Beach Obstetrics & Gynecology of Palm Beach, Florida implemented an EHR system that integrated scheduling and charting while also handling such business functions as billing, collections, and reporting. Overall practice efficiency increased significantly; so did staff and patient satisfaction. According to Managing Partner, Sam Lederman, MD, "The system has paid for itself several times over in practice efficiency and cost savings."[10]

Most recently, a March 2013 study published in *Health Affairs* and detailing results from a survey of 49 physician practices in Massachusetts, found the following: Those practices generating a positive ROI from their EHR implementation increased revenue by an average of more than $114,000 per physician over five years.[11]

Risks

In addition to the operational risk inherent in any IT implementation, EHR implementation also includes HIPAA-related risks. As you know, all activities involving EHR and personal health information (PHI) must be conducted in compliance with HIPAA. Signed into law in 1996 and with penalties in effect since 2005, enforcement of HIPAA Privacy Rules had, until recently, been lax.

With the passage of the HITECH Act though, steps were taken to toughen laws, stiffen penalties and step up enforcement. What was once a relatively harmless HIPAA stick ($100 per violation with a $25,000 maximum per year) is now a much more punishing HIPAA club. Most recently, in January 2013 the penalty for HIPAA violations was increased to a maximum of $1.5 million per incident.[12] The most severe penalties are reserved for violations determined to have occurred as a result of "willful neglect." The HITECH Act defines willful neglect as:

> "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated."[13]

What was once a relatively harmless HIPAA stick ($100 per violation with a $25,000 maximum per year) is now a much more punishing HIPAA club.

The final text of the legislation includes specific examples of the type of activities that constitute willful neglect violations. Each of these examples illustrates that the covered entities:

1. Had "actual or constructive knowledge of their various violations"
2. Failed to develop or implement compliant policies and procedures or to respond to incidents, thus demonstrating "either conscious intent or reckless disregard with respect to their compliance obligations."[14]

The HITECH Breach Notification Rule requires covered entities to report any PHI breach of 500 or more individuals to the Secretary of HHS and the media within

60 days of discovery. Breaches affecting fewer than 500 people must be reported to the Secretary annually.

HHS swings the HIPAA club: Recent violations and civil money penalties imposed

As the following actions show, the U.S. Department of Health & Human Services (HHS) is now quite serious about HIPAA enforcement:

- In February of 2011 HHS imposed a civil money penalty of $4.3 million against Cignet Health of Prince George's County, Md. for violation of HIPAA privacy rules.[15]
- In early 2011, General Hospital Corporation and Massachusetts General Physicians Organization Inc. agreed to pay $1,000,000 to settle potential HIPAA privacy violations.[16]
- In July 2011, the UCLA Health System agreed to settle potential HIPAA privacy violations for $865,500.[17]

And lest one think that HHS has restricted its HIPAA enforcement activities to only the larger healthcare organizations there are these two recent actions:

- In April 2012 Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona agreed to pay HHS a $100,000 settlement for failing to take adequate actions to safeguard the protected health information of its patients. A report that the physician practice was posting its patients' clinical and surgical appointments on a publicly accessible Internet-based calendar triggered the HHS investigation. The practice was also cited for four additional noncompliance issues, including failure to obtain business associate agreements with IT service providers.[18]
- In January 2013, the Hospice of North Idaho (HONI) agreed to pay HHS $50,000 to settle potential HIPPA violations. HONI had reported that one of its unencrypted laptop computers containing the electronic protected health information of 441 patients had been stolen.[19]

In April 2012 Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona agreed to pay HHS a $100,000 settlement for failing to take adequate actions to safeguard the protected health information of its patients.

Pointedly, the news release announcing the HONI breach settlement includes the following quote from an HHS official: "This action sends a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information."[20]

Covered entities and business associates

Under HIPAA Privacy rules the term "covered entity" refers to three specific groups: health care providers, health plans and health care clearinghouses. With few exceptions all entities within these groups are subject to HIPAA Privacy rules.

Also, as part of the HITECH Act the definition of covered entity extends to all business associates of the covered entity as well as any subcontractors to these business associates. HHS defines a "business associate" as follows:

> "In general, a business associate is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information."[21]

The key phrase is "involve the use or disclosure of individually identifiable health information." Without such activity there is no "business associate" relationship defined by the HITECH Act.

Technical competence and a detailed business associate agreement. Two keys to ensuring a successful HIT implementation and HIPAA/HITECH compliance.

During NetGain Technologies' 28 years of operation it's been our experience that small and mid-size healthcare organizations don't often maintain the full complement of IT staff needed to implement major HIT upgrades. This is understandable. Small and mid-size healthcare organizations have more limited resources and their day-to-day IT needs are usually not demanding enough to justify a large, full-time IT staff.

Given the favorable forces currently at work though, smaller healthcare organizations are seeking out experienced, specialized help to assist them with EHR implementation and other HIT upgrades. But healthcare organizations must not only conduct their due diligence with an eye for technical competence, they must also cast an equally critical eye upon each prospective vendor's knowledge and capabilities regarding HIPAA/HITECH compliance.

For example, take the HHS action against Phoenix Cardiac Surgery, P.C., referenced earlier. One of the four additional noncompliance issues for which it was cited was failure "to obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI."[22]

Obviously, the email and calendar services vendor that did the work was technically competent. Patient appointments were, after all, able to be posted and publicly accessed through an Internet-based calendar. On the other hand, the vendor demonstrated a costly lack of knowledge about HIPAA Privacy Rules. Otherwise it would never have set up the calendar the way it did. And it would never have commenced the project in the first place without a signed Business Associate Agreement.

A Business Associate Agreement (BAA) obligates the contracting party –

for instance, a health IT solutions provider – to "implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that they create, receive, maintain, or transmit on behalf of the covered entity as required by the Security Rule...."[23] The preceding terms also apply to any subcontractors of the Business Associate that in the course of their work on behalf of the Business Associate may come in contact with PHI.

Important verbiage that every BAA should have:

The BAA should categorically state that the performance of the agreement may involve "protected health information" and explicitly tie definition of the term to a codified federal regulation (CFR).

Example: Performance of the Underlying Agreement may involve Protected Health Information (as defined in 45 CFR § 164.501) that is subject to the federal privacy regulations issued pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and codified at 45 CFR parts 160 and 164 (the "Privacy Rule").

The BAA should categorically state that the performance of the agreement may involve "protected health information" and explicitly tie definition of the term to a codified federal regulation (CFR).

HIPAA Security Rule

Every potential partner should be compliant with the HIPAA Security Rule. Essentially a subset of HIPAA Privacy Rules, the HIPAA Security Rule deals with electronic PHI (ePHI). The HIPAA Security Rule defines national standards for protecting ePHI and dictates that all covered entities (and by extension, their business associates) provide administrative, technical, and physical safeguards to prevent the unauthorized access and transmission of ePHI:

- Administrative safeguards define and detail the standards and specifications for a covered entity's health information security program
- Physical safeguards define and detail the physical barriers and other preventative measures that control physical access to a covered entity's office and computer systems as well as locks and alarms that ensure only authorized personnel have access to systems and data
- Technical safeguards define and detail the hardware, software and related technology that limit unauthorized access and transmission of ePHI, including access, audit and integrity controls and transmission security measures.

Ask any potential partner about the specific actions it has taken to provide administrative, technical and physical safeguards against unauthorized access and transmission of ePHI.

Ask any potential partner about the specific actions it has taken to provide administrative, technical and physical safeguards against unauthorized access and transmission of ePHI.

Is the Partner audit-ready?

As noted earlier, healthcare organizations must carry out their HIT vendor search with a keen eye for both technical competence and HIPAA/HITECH compliance capabilities. Ideally, any partner you consider will have several years of experience in the healthcare industry, a track record of success, and sterling references. Ideally, it will have made a commitment – administratively, physically and technically – to safeguarding PHI; and made this an ongoing, day-to-day commitment. Ideally, it already has everything in place, administratively, physically and technically to be HHS audit-ready because that day is coming, sooner rather than later.

As noted in section 13411 of the HITECH Act, HHS is required to periodically audit the compliance of HIPAA-covered entities and their business associates with the Privacy, Security and Breach Notification rules. In fact, from November 2011 – December 2012 piloted an audit program by conducting 115 such audits.

Screening potential IT Partners for your healthcare organization: Six important questions you need to ask.

If you're actively engaged in a search for a health IT partner you don't want to waste time with any firm that's not HIPAA/HITECH-knowledgeable. With this thought in mind, here are six straightforward questions to ask that potential partner's Service Operations Manager, the answer to any one of which can eliminate unqualified partners and save you a lot of time:

1. **"Will you sign a BAA with my organization?"** If there is any hesitation, if the answer is anything but an unqualified "yes" drop the company from consideration.

2. **"Can you email me a copy of your standard Business Associate Agreement?"** If the answer is anything but an unqualified "yes" drop the company from consideration. Furthermore, if the promised email doesn't hit your inbox within 24 hours (and preferably sooner), drop the company from consideration. Because if it can't comply with your request within 24 hours it's highly likely it doesn't have a standard Business Associate Agreement for its clients. If it doesn't, it's a sure sign that the company and its executives are not HIPAA/HITECH-knowledgeable.

3. **"Can you give me the name of your HIPAA Privacy Official?"** If this name is not immediately offered to you drop the company from consideration; because this company obviously does not have a HIPAA Privacy Official.

4. **"Can I see a copy of your HIPAA Documentation? Again, if the answer is anything but an unqualified "yes,"** drop the company from consideration. If the answer is yes you need to look for the following:

a. More than 50 clearly defined HIPAA Policies and Procedures

b. 3rd party certificates for BA training for each appropriate member of its staff.

If you don't see both "a" and "b" drop the company from consideration.

5. **"Can I see your company's written policy on continuous staff training and documentation of staff training for the most recent six month?"** This is where most IT organizations pretending to know HIPAA fail. If the company can't produce this information for you in short order, drop it from consideration.

6. **"How long have you been in business and will you show my accounting person your company's financial records?"** Sure, this is two questions in one. But since most businesses fail within the first five years, you want a partner that has been in business a minimum of five years – the longer, the better. As for financials, you need to know your potential IT partner is a healthy company. Otherwise, you may find yourself without the service you expect and an inability to use their financial strength to accomplish what you need throughout the life of your relationship.

The rewards of successful implementation and ongoing use of health information technology are many and substantial, as are the risks of HIPAA non-compliance.

Summary

As arduous and time-consuming as the health IT partner selection process is, it makes sense to make every effort to select a partner that you can trust and depend upon for the foreseeable future. The rewards of successful implementation and ongoing use of health information technology are many and substantial, as are the risks of HIPAA non-compliance. To reap the benefits of the former and avoid potential losses from the latter, look for a partner with a proven track record of technical competence and a keen understanding of what it takes – administratively, physically and technically – to run a HIPAA/HITECH-compliant IT services organization.

How secure is your PHI? Can your healthcare organization benefit from a complimentary security assessment?

For more than 15 years NetGain Technologies has been partnering with small and mid-size healthcare organizations to lock in HIT benefits while providing lock-down security for patient records. During this time we've learned a thing or twenty about HIPAA compliance, from both a regulatory perspective and an operational perspective. Simply put, we've made it our business to be subject matter experts on HIT and HIPAA compliance. And we'd like to share our expertise with you. To this end, we are offering you and your organization a complimentary security assessment. This complimentary security assessment includes a personal meeting at your office with one of our experienced and knowledgeable HIT consultants.

Your NetGain Technologies consultant will review specific HITECH Security and Privacy requirements that must be met in order to establish and maintain HIPAA compliance. As part of this review, questions will be posed about your organization's policies and procedures regarding PHI security. These questions will pertain to important HIPAA concerns such as –

- Documentation of, and employee access to, HIPAA policy and procedures
- Organization policies and procedures pertaining to HIPAA training and certification of training
- Encryption of ePHI data and storage of ePHI data off-site
- Workstation use and security policy,

and more.

If you're like most healthcare professionals we've conducted these assessments for, you'll come away from this meeting either reassured that you have everything under control or better informed about specific steps you need to take. Either way, we believe you'll find it to have been a worthwhile investment of your time, usually 30 – 60 minutes.

To schedule your security assessment contact us today at 1.866.367.7243 or email us at SecurityAssessment@NetGainIT.com

Endnotes:

[1] "The Benefits Of Health Information Technology: A review Of The Recent Literature Shows Predominantly Positive Results." Health Affairs,30 no. 3 (2011): 464-471 http://www.ilhitrec.org/ilhitrec/interchange/july_2011/benefits.pdf Melinda Beeuwkes Buntin, Matthew F. Burke, Michael C. Hoaglin and David Blumenthal.

[2] Ibid.

[3] "Data and Program Reports" CMS.gov http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/DataAndReports.html "Electronic Health Records in Ambulatory Care – A National Survey of Physicians."

[4] DesRoches CM, et al. http://www.ncbi.nlm.nih.gov/pubmed/18565855 New England Journal of Medicine. 2008. "Physician Adoption of Electronic Health Record Systems: United States, 2011."

[5] Jamoom, E, et al. NHCS Data Brief No. 98, 2012.

[6] "How will adopting electronic health records improve my ability to care for patients?" http://www.healthit.gov/providers-professionals/faqs/how-will-adopting-electronic-health-records-ehr-improve-providers%E2%80%99-abil

[7] "The Value Of Electronic Health Records In Solo Or Small Group Practices" http://content.healthaffairs.org/content/24/5/1127.full.html Robert H. Miller, Christopher West, Tiffany Martin Brown, Ida Sim and Chris Ganchoff

[8] "A Pilot Study to Document the Return on Investment for Implementing an Ambulatory Electronic Health Record at an Academic Medical Center" Journal of the American College

of Surgeons Volume 205, Issue 1 , Pages 89-96, July 2007 http://www.journalacs.org/article/PIIS1072751507003900/abstract

[9] HIMSS Electronic Health Record (EHR) Association web site. http://www.himssehra.org/docs/caseStudies/eClinicalWorks_MSSNY-3.08-b.pdf

[10] "HIT Journeys" HealthIT.gov web site. http://www.healthit.gov/providers-professionals/implementing-EHR/palm-beach-obstetrics-gynecology-pa

[11] "Most Physicians Lose Money After Adopting EHRs, New Study Finds" March 05, 2013 iHealthBeat web site, a service of the California HealthCare Foundation http://www.ihealthbeat.org/articles/2013/3/5/most-physicians-lose-money-after-adopting-ehrs-new-study-finds.aspx

[12] "New rule protects patient privacy, secures health information." January 17, 2013 U.S. Department of Health & Human Services news release. http://www.hhs.gov/news/press/2013pres/01/20130117b.html

[13] 45 CFR Parts 160 and 164, Section III F. Subpart D—Imposition of Civil Money Penalties, Section 160.401 Definitions http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/nprmhitech.pdf

[14] Ibid.

[15] "HHS imposes a $4.3 million civil money penalty for violations of the HIPAA Privacy Rule." February 22, 2011 U.S. Department of Health & Human Services news release. http://www.hhs.gov/news/press/2011pres/02/20110222a.html

[16] "Massachusetts General Hospital settles potential HIPAA violations." February 24, 2011 U.S. Department of Health & Human Services news release. http://www.hhs.gov/news/press/2011pres/02/20110224b.html

[17] "University of California settles HIPAA Privacy and Security case involving UCLA Health System facilities." July 7, 2011 U.S. Department of Health & Human Services news release. http://www.hhs.gov/news/press/2011pres/07/20110707a.html

[18] "HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards." April 17, 2012 U.S. Department of Health & Human Services news release. http://www.hhs.gov/news/press/2012pres/04/20120417a.html

[19] "HHS announces first HIPAA breach settlement involving less than 500 patients" January 2, 2013 U.S. Department of Health & Human Services news release. http://www.hhs.gov/news/press/2013pres/01/20130102a.html

[20] Ibid.

[21] "Summary of the HIPAA Privacy Rule" U.S. Department of Health & Human Services web site. http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

[22] Ibid. 18

[23] "A Rule by the Health and Human Services Department on 01/25/2013" https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the