Friendly Customers!
Friendly Connections!
Friendly Computers!

June 2013

Technology Today

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"**- Bill Schubert, Friendly Computers**

Inside This Issue...

Next Month's Issue:

Next month we get back to our usual collection of IT information useful to everyone. But I will keep an eye on the HIPAA landscape including something in each issue as things change. The environment is rapidly changing. I'll try to keep things up to date here in Technology Today.

Bill

HITEC/HIPAA Special Edition

From the Editor:

Friendly Computers has a number of health care providers we support. As a result we have focused on two areas in the new HIPAA arena. First is to get our house in order. We have been working, since the first of the year, towards tightening up our own security to meet the HHS guidelines. This has the added benefit of ensuring Friendly Computers meets or exceeds the many other security requirements such as PCI Compliance and Sarbanes-Oxley. We are spending a lot more time thinking, reading and writing about security these days. This leads to the second result which is applying what we know about computer systems security in the HIPAA world to help our customers. This newsletter is hopefully a bit of that help. It is a compilation of some of the best information I can find with, hopefully, a useful explanation of what needs to be done. Please contact us with any questions and of course if we can help you.

Bill Schubert

Note (Even HHS puts a disclaimer on their site.): None of the information here should be construed as advice to be taken without verifying its accuracy and legality with your attorney.

What does this have to do with me? Our company is not medical?

The new HIPAA rules (part of what is know as the HIPAA Omnibus rule which is actually a number of different rules governing the conduct of healthcare patient information management) have changed the playing field in a number of ways, the most important of which from the standpoint of a non-healthcare provider business is that of responsibility shift. In this case we're looking at the " Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164. " Until the first of 2013 the responsibility for ensuring that any contractor or Business Associate (BA) who had or might have access to patient health information has sufficient training and security awareness was almost entirely on the provider. Lawyers, CPA's, information support services and all of the vendors who interact with a practice have the potential to be classified by Health and Human Services to be BA's and as such are now liable to audit and are responsible for their own training and security.

The list of businesses that fall within the HHS audit window is a little vague so some care is required if you do business with a Health Care provider at all.

See page 2 for further information about the BA process.

If you interact with a Health Care Provider...

If your business interacts with a health care provider on any level it is worth considering what might happen if the Office of Civil Rights (or the Health and Human Services enforcement branch) should send you a letter asking about your compliance.

Compliance with the law must be completed by the 23rd of September of this year. Meeting the very thorough compliance requirements is now the cost of doing business. Not meeting them may result in some significant momentary penalties not the least of which is loss of access to work with any other health care provider.

There are a number of vendors who, for a reasonable cost, will help ensure Business Associate compliance. The OCR budget has increased sufficiently that a 5% audit of eligible covered entities is anticipated. Business Associates are not exactly in the cross hairs but there is obviously serious liability involved. Certainly any BA that actually has access to patient data should be very concerned and should be proactively conducting the necessary internal audits and training required to gain and maintain compliance.

Even businesses who to not maintain patient data on their systems but do interact with health care providers can and should look at their processes and training to ensure that they understand the HIPAA patient information protections. Meeting such stringent requirements also means that information security overall is better.

Friendly Computers of Georgetown can help with both the procedural and physical process of compliance. We work with two excellent specialists and can ensure that you are audit safe as efficiently as possible.

The top 10 things you need to know and do

1: Physical security policies

These policies should specify who is and isn't allowed physical access to your facilities and equipment. This could include a policy on guests entering your premises, what staff members have access to server rooms, and who is authorized to get into the executive wing. Once you have the policies, your procedures should describe how you enforce your policies. For small businesses the space access control is easier but no less important.

2: Access control

There should be specific policies and procedures on how users are granted access to programs, sensitive data, or equipment. This includes how access is requested and authorized, how administrators are notified to disable accounts when appropriate, frequency of account audits, and how records of all this activity are maintained. If your computers are not on a domain it might be a good time to think about doing that. Having security policies on a domain is really the only way to monitor activity with any certainty.

3: Workstation use policies

This is a fairly broad topic and includes some of the most basic system safeguards: limiting unsuccessful login attempts, monitoring login records, and requiring passwords to be of an appropriate strength and to be changed regularly. This should also include policies on how the equipment is used, such as mandating that users not write down their passwords or share them with other employees.

4: Security awareness

A security awareness and training program should be put in place that encompasses everyone in the organization. This should include programs for new hires, annual training, and periodic security reminders. I send security updates to all staff with information about some of the latest threats and concerns. I particularly like to send out screenshots of notable phishing attacks and compromised Web sites to raise awareness. It is crucial that you keep an audit trail of your reminders.

5: Malicious software

Of course you have antivirus software installed. But do you have documented policies and procedures for when and how often virus definitions are updated? Do you have a response procedure for a virus outbreak? How about staff policies on reporting detected viruses, not opening attachments from unknown senders, and not disabling the software? Cloud based antivirus solutions such as the one we use and support, AVG Cloudcare provide an excellent centralized management of this environment.

Backup and Disaster Recovery

One of the critical aspects of HITEC/HIPAA happens to be critical and also frequently ignored by small businesses, BDR. While these days nearly all businesses run some kind of backup, very few actually assess the level of information "insurance" they need to hedge against a disaster and maintain their business continuity.

Some fairly new systems are available that can be set in place which make nearly bulletproof both disaster recovery (if the building were to burn down) and business continuity (loss of either building or just the server). Where in the past it would cost thousands of dollars a month to set up such a high end solution that is no longer the case.

For less than $300/month most systems can be backed up in such a way that a loss of server might result in only an hour's down time while loss of the entire structure might result in only a day's loss of capability. Images of the server can be made up to 4 times per hour and the entire server can be recovered in minutes remotely by a remotely located technician.

Give us a call at Friendly Computers to discuss this iron-clad BDR!

6: Disaster recovery

and

7: Business continuity

Policies and procedures should be in place for responding to an emergency. This includes small emergencies, such as a server going down, as well as large emergencies, such as prolonged power outages or fires.

See BDR discussion in the left hand column.

8: Media disposal

Medial disposal is one of many additional areas that need to be addressed. I included it, though, because I am asked about it frequently. A common concern is data that lives on equipment other than computers: copiers, smartphones, and even fax-machines (in case you still have one somewhere). We have policies and procedures in place that mandate how we wipe the data off each kind of storage media and how these activities are logged.

9: Risk analysis

I found this to be the most interesting of the areas discussed here. At a very high level, a process is needed to identify risks and the controls that are in place to mitigate them. Under HIPAA, the primary concern is risk to systems and processes that deal with health information, although it can be extended to any part of the organization. Ultimately, every other item on this list is really a control to mitigate against risk.

There are plenty of good online resources to assist in developing a risk analysis and management strategy. I recommend the National Institute of Standards and Technology's publication on Risk Management for IT Systems. A well-documented risk analysis and management program will include the process by which risks are identified, as well as the process for establishing and executing action plans in response.

10: Review and audit procedure

Every item on this list has a couple of things in common: First, it must be auditable. You don't get credit unless there is a documented audit log that shows that these procedures are being executed. There also needs to be a process that ensures that the policies and procedures are reviewed regularly. And when you review a policy or procedure and find that it needs to be updated? Well, you need a policy and a procedure for that.

The Lighter Side:

HIPAA Puns *

What's the effect of most HIPAA presentations?
HIPAA-nosis

What do you call someone who preaches privacy, but doesn't follow through?
HIPAA-critical

What do you call a provider if he/she is found to have violated patient confidentiality?
HIPAA-cratic HIPAA-crit

What do you call a theory for HIPAA success?
HIPAA-thesis

What do you call the complete understanding of all HIPAA rules?
HIPAA-thetical situation

If you've heard about HIPAA compliance until you're blue, you might be:
HIPAA-thermic

What do you call someone who complains incessantly about HIPAA?
HIPAA-chondriac

If you're sure you know all the HIPAA rules, you're probably:
HIPAA-go-lucky

Who was the first Privacy Officer in the Old West?
HIPAA-long Cassidy

What do you call someone who is afraid of HIPAA?
HIPAA-phobic

What do you call a boring person who talks in circles about HIPAA?
HIPAA-drone

*Thanks to the University of Florida for the puns.

Secure Off-site Storage

What are the rules? Can I use Dropbox (or anything like that)? What about off-site backups?

The rules for both of these are similar and it brings up some interesting points. Physical storage of records points the way:

"Storage" Creates a BA Relationship: *Where do you store your old medical records? Lots of small practices rent a self-storage unit somewhere to keep boxes of old paper medical records. Those storage facilities don't consider themselves to be in the "medical record storage" business, don't intend to access the records, don't "maintain" them in the traditional sense of the word, don't have policies and procedures or other safeguards in place (other than locks on the doors), and probably won't be willing to sign a business associate agreement (or if they sign one, probably wouldn't do a good job of complying with it). In common-law terms, there is no "bailment," and they don't consider themselves to be bailees. Under the original HIPAA rules, they had a very strong argument that they were not business associates.*

However, under the Omnibus Rule, they almost certainly are business associates. Even if they protest and deny any intent to become one, they probably still are. "Conduits" such as the post office, FedEx and UPS get a special exception, but storage companies don't.
Jeff Drummond, hipaablog

The storage of data (as opposed to the transmission of data) creates a Business Associate relationship. Meaning that if a health care provider puts patient information in an email and sends it the carrier (Verizon, Suddenlink, ATT, etc) is not a BA but the email server (for instance, Microsoft) is a BA. This means that the health care provider using a Microsoft service that might end up with patient data on it at some point should get an agreement letter from them. Microsoft has, in fact, agreed with this and has made itself available to provide signed agreement letters (BAA) with its customers in the case of Office 365 and all of their other online (cloud) services.

In a press release on 25 April:

Microsoft Corp. today announced the release of a new, revised version of its HIPAA Business Associate Agreement (BAA) for the company's next-generation cloud services. This enables customers in the healthcare industry to leverage cloud solutions to coordinate care, improve patient health outcomes, and maintain compliance with privacy and security regulations issued under the U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996.

This puts them out ahead of most of the other solution providers such as Google and Amazon who will not (so far) sign a BAA.

But, wait, I need to answer the question. Actually, Dropbox is not, as of May 2013, HIPAA compliant. Box.com is a similar service that is developing a specialty in HIPAA and health care and is compliant. There are others but Box.com leads the group right now.