HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

December 15, 2015

Volume 1, Issue 12

Uninformed About Business Associates?

I have been in a few new medical offices lately chatting with Practice Administrators about computers and IT. I am picking up on a disturbing common theme. Not everyone understands the definition of a Business Associate and their obligations to the Practice, especially when it comes to their IT firms.

To make a long story short, Computer and Information Technology companies are Business Associates because they have access to, or are in possession of, Protected Health Information (PHI).

Under the Omnibus Final Rule (January 2013), a "Business Associate" is generally a person or entity that creates, receives, maintains, or transmits protected health information (PHI) in fulfilling certain functions or activities for a HIPAA-Covered Entity.

Also, the new definition clarifies that "Business Associates" include entities that "maintain" PHI for a covered entity, such as a data storage company for offsite backups.

Business Associates and their subcontractors have the same basic obligations to protect PHI as a Covered Entity (CE).

The Final Rule implements HITECH's requirements for Business Associates to directly comply with parts of the Security Rule. For example, under the Final Rule, the Security Rule requires Business Associates to ensure the confidentiality, integrity and availability of electronic PHI that the Business Associate creates, receives, maintains or transmits, and also to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI. The Final Rule also directly requires a Business Associate to adopt certain security measures to implement the standards and implementation specifications under the Security Rule, including specific **administrative safeguards, physical safeguards and technical safeguards**.

Business Associates must also conduct a Security Risk Analysis, assess the risks and vulnerabilities of electronic PHI, and remediate any problems found.

What Does This Mean To You?

If you hire an outsourced IT company, they have to do all the same things as you to protect patient PHI. It does not matter if the outsourced IT firm is a single person firm, or if they number in the hundreds, **they all have to comply**.

Compliance means:

- Security Risk Analysis (SRA)
- Remediate any issues found during the SRA
- Develop Polices and Procedures
- Conduct Staff Training
- Sign a Business Associate Agreement with all the Omnibus changes (dated after January 25, 2013)

Your IT firm should have no problems showing you a copy of their Security Risk Analysis, their Policies and Procedures and their staff training certificates. Obviously, they should carry Errors and Omissions insurance on top of the other standard insurances a typical business carries.

Health and Human Services (HHS) and the Office for Civil Rights (OCR) have indicated that they will conduct 1,200 audits this year. During those audits they intend to ask the Covered Entities for their Business Associate Agreements. Then OCR plans on auditing the Business Associates and the BA's subcontractors for compliance. **If the BA fails, you (the CE) fail!**

If your IT firm cannot prove to you beyond a shadow of a doubt that they are compliant, then

you are required to terminate your relationship with them.

This is some serious stuff. You might have been able to stick your head in the sand up until now but the government is about to crack down…and you do NOT want to the one they crack down on. The potential fines are huge and the newspaper and media exposure is not the type of thing we want our Patients reading about. It has a tendency to destroy the trust between the Patient and the Practice.

You know where to find me:
Rick Boyles
757-333-3299 x200
rick.boyles@computernetworksinc.com

Sack of Potatoes

Some of you might not know me from a sack of potatoes, so I am going to take a couple of minutes to bring you up to speed:

1997 – 1998	**Medic Computer Systems** Field Engineer
1998 – 2001	**Misys Healthcare (purchased Medic)** Virginia Beach Branch Manager-Field Engineering
2001 – 2004	**Misys Healthcare** Advanced Implementation Services Engineer-1 of 7 in the U.S. charged with successful implementing Misys EMR/EHRs
2004 – 2015	**Founder Computer Networks, Inc.** Healthcare Information Technology Computer Support HIPAA Risk Analyses Disaster Recovery

So, if you do the math, I have been in Healthcare Information Technology for the past 18 years, 11 of them as Owner of my own firm.

If you take a peek around at some of the other IT firms in our area, you will see that they do not specialize in Healthcare IT, that their Owners/Founders do not have a background in Healthcare IT, and consequently do not always understand the challenges presented in Healthcare. ☸

Business Associate Examples

- An outsourced Computer firm/IT firm.
- A document shredding company.
- 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 protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- 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.☸

http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

December 15, 2015

Volume 1, Issue 12

I Am So Confused Who Is NOT A Business Associate?

•A provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other.
•With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be **incidental**, if at all.
•With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers (UPS, FEDEX), and their electronic equivalents (Internet Service Providers).
•Among covered entities who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA.
•Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA, with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA.
•Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the covered entity purchases the insurance benefits, and when the covered entity submits a claim to the insurer and the insurer pays the claim.
•To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.
•When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.❁

Just Make It All Go Away!

NEW! 36 Month HIPAA Compliance Plan

36 months of HIPAA compliance consulting (includes a complete, onsite, Security Risk Analysis with Remediation Plan, quarterly network scans for 3 years, Policy and Procedure templates including guidance on implementing, incident investigation, breach investigations, unlimited HIPAA compliance questions) for one low monthly fee. Ask, call, or email me for details!

PHI is everywhere. Find it. Protect it. ❁

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

December 15, 2015

Volume 1, Issue 12

My Practice Is Too Small

They Will Never Catch Me

•Triple-S Management Corporation Settles HHS Charges by Agreeing to $3.5 Million HIPAA Settlement - November 30, 2015

•HIPAA Settlement Reinforces Lessons for Users of Medical Devices - November 24, 2015

•$750,000 HIPAA Settlement Emphasizes the Importance of Risk Analysis and Device and Media Control Policies - August 31, 2015

•HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications - June 10, 2015

•HIPAA Settlement Highlights the Continuing Importance of Secure Disposal of Paper Medical Records - April 22, 2015

•HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software - December 2, 2014

•$800,000 HIPAA Settlement in Medical Records Dumping Case - June 23, 2014

•Data Breach Results in $4.8 Million HIPAA Settlements - May 7, 2014

•Concentra Settles HIPAA Case for $1,725,220 - April 22, 2014

•QCA Settles HIPAA Case for $250,000 – April 22, 2014

•County Government Settles Potential HIPAA Violations - March 7, 2014

•Resolution Agreement with Adult & Pediatric Dermatology, P.C. of Massachusetts - December 20, 2013

•HHS Settles with Health Plan in Photocopier Breach Case - August 14, 2013

Proceed at your own risk…

Plug The Holes

The Security Risk Analysis is about identifying the areas of your Practice where Patient information (PHI) might leak out and then plugging those holes. It is a bit of a burden to do the first one, but, after that it is a matter of staying on top of any changes to your Practice that might open up a leakage of data to the outside world.

It is not a huge undertaking when you have done a few of these, but, if you are at your first rodeo, then the process is generally overwhelming. That is why we are here to help.

You cannot continue to ignore the responsibilities of the Practice to protect the Patient's PHI.

You can throw up your hands and sell yourself to a hospital, but, the first thing they are going to do is make you become HIPAA compliant. So, that is not the way to solve the problem! It is just going to jump back into your lap unless you retire at the time of the sale.

None of us in this market like the rules. But, the rules are the law and few, if any, of us want to be lawbreakers. Plus, we have a duty to protect the income stream of the Physician Owner(s) of the Practice. Getting socked with a couple hundred thousand dollar fine for not taking the time to get compliant is not doing a good job of protecting the Doctor and his livelihood.

If you want to talk HIPAA, let me know. We are scheduling Security Risk Assessments for January now. ☸