



HIPAA and HITECH Affects the Call Center

By Charlene Glorieux, ATSI executive vice president

If you deal with medical accounts, significant changes are coming, and coming quickly as you may well know. Not only is the ARRA (Stimulus Act) pumping millions of dollars into the healthcare industry in a quick dash to overall conversion to Electronic Health Records (EHR), but it also imposes a whole new set of rules upon Covered Entities (CE) and Business Associate (BA)s. HIPAA as we knew it has dramatically changed its face. TASs which use protected health information (PHI) to provide services to clients will have to change the way they do business. You may have already seen some of this reflected in a flurry of proposed new Business Associate Contracts (BAC) from your medical clients.

The HITECH Act impacts Covered Entities and their Business Associates. Gone are the days when the CE had all the responsibility and liability for any disclosures of PHI; BAs like TASs now are also directly responsible and liable for any failures on their part – or even for knowing about a breach within the CE and not reporting it!

You need to be HIPAA/HITECH compliant! Your industry competition WILL be and your covered entity clients MUST have assurances that you have addressed these requirements or they will be looking elsewhere; there is too much at stake for them otherwise.

Hold on – help is on the way!

ATSI's Government Relations HIPAA Subcommittee has been working to clarify the impact that HITECH/ARRA is making on our industry and to prepare its members for the February 17, 2010 implementation date. Projects being undertaken include: HIPAA/HITECH Privacy and Security Rule guidance resources; a sample letter to clients; model BACs for clients; model vendor/service provider contracts; model HIPAA policies; documentation tools; compliance training programs for frontline staff as well as for managers and owners (two very different types of training); and a review of ATSI's Errors and Omissions insurance program as well as General Liability insurance for enhanced coverage.

The Details

First, you are not a Covered Entity and you should be glad! HIPAA imposes much greater requirements on CEs than on Business Associates, though both face similar penalties. Covered entities under the HIPAA Rules are health plans, health care clearing houses, or health care providers that transmit any health information electronically in connection with a covered transaction.

Second, in order to even be considered a Business Associate, you must be using PHI to provide a service to your client. PHI under HIPAA means any information that identifies an individual *and also* relates to at least one of the following:

- The individual's past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

Information is deemed to identify an individual if it includes either the individual's name or any other information that could enable someone to determine the individual's identity.

PHI might be in use if you offer services such as switchboard overflow services, after hours urgent messaging, daytime urgent and non-urgent messaging, outbound follow-up calls, pre-op instructions, centralized physician referral, appointment scheduling, appointment and other kinds of reminders, test results etc.

If you are indeed a BA, then you must have a detailed BAC with your client CE. The BAC must comply with the requirements of HIPAA but none of it should create obligations on your part in excess of what is required by HIPAA. However, it must include the additional requirements relating to the HITECH act.

So what does HIPAA/HITECH require of a Business Associate? The biggest changes to affect Business Associates are:

1. The HIPAA safeguards now apply to the BA in nearly the same manner as the CE. BAs must now comply with all the enhanced administrative, technical and physical safeguards as well as policy, procedure and documentation requirements of the Rule.
2. BAs have mandatory breach reporting requirements and have both responsibility and liability for breaches. This can include exposure to civil suits from those individuals who had their PHI breached while in the custody of the CE.
3. BAs are now subject to the same criminal and civil penalties as CEs for breaches of unsecured protected health information. Breaches can be quite costly; you can lose your client and be exposed to criminal and civil penalties.

4. The specific, applicable security requirements of the HIPAA Security Rule must be incorporated into the BAC between a CE and their BA.

Policy, Procedure and Documentation

The HITECH Act requires BAs to revise many of their policies and procedures to comply with the HIPAA Privacy and Security Rules. And of course, these must be documented in the event of an audit.

If you do not already have these you will need to create compliant policies for areas such as: systems and network security, data storage practices, privacy practices, accounting for disclosures, breach reporting, remote operations, etc. Some of this is basic good business security and you might already have it; others may need to be created for the first time.

You should do a risk assessment of your systems (where and when are they vulnerable), your physical set up (could a visitor to your operation see or overhear enough to constitute a breach, are your computing assets physically secure), your training programs, your documentation policies and any other potentially vulnerable area.

Business Associate Contract

A Business Associate Contract (BAC) is a new term commonly used to describe what we used to know as a Business Associate Agreement (BAA). In 2003, at the time the HIPAA Privacy Rule first took effect, ATSI crafted a simple, straight forward Business Associate Agreement for its members' use which eliminated the onerous and unnecessary clauses many client CEs attempted to insert which attempted to pass the CEs liability onto the Business Associate as well. Again, in 2005, ATSI revised and updated the model BAAs upon the imposition of the HIPAA Security Rule. ATSI members had great success using these model BAAs, and ATSI will be providing a newly revised model BAC before the February 2010 deadline. The model BAC will include only the language that is required under HIPAA/HITECH.

Training Requirements

Those of us handling PHI are already training our staff in HIPAA privacy and security, but there needs to be ongoing training that keeps abreast of the changes that are happening to the Rules now and are likely to continue to happen as the requirements of HIPAA and HITECH are further refined through use. Verifiable, ongoing, correct training that adapts to these changes as they come along will be necessary for your staff, as well as the means to document that they have participated in the training.

Managers and owners will also need training to ensure they are knowledgeable about the myriad of requirements that have now been imposed directly upon Business Associates by ARRA and HITECH. You will need a compliance officer to keep on top of these issues within your company. Once again, the requirements are likely to change over the next few years and you should make every effort to keep informed of the latest developments and adjust your operations accordingly.

There are many canned compliance training programs available for sale now, but they primarily address CEs and other BAs with a high degree of PHI use. ATSI members will have access to industry-specific training for frontline staff, managers and owners available prior to the February implementation deadline. These programs will be updated regularly as the law and regulations change and will be specially priced for the unique needs of our industry.

Breach Notification & Reporting Requirements

The main concern here is a breach of unsecured PHI. Unsecured PHI is PHI that the CE or BA has not secured via standards approved by the Secretary of Health and Human Services. A breach is defined as “the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.”

If you have a breach of unsecured PHI, for example a hacker gains access to the your systems, you must report this breach to your client CE “without unreasonable delay” but no later than 60 days from the discovery of the breach – OR from when the breach should have been discovered by your exercising reasonable diligence. If you wait the full 60 days, you better have a good reason for the delay.

If you are using the specified technologies and methodologies approved by the Secretary (encryption and destruction) then you do not have unsecured PHI and you don't have to report a breach of the properly secured PHI! This doesn't mean you HAVE to use these technologies and methodologies; the Security Rule permits the use of other access controls to make the information inaccessible, but a breach of unsecured PHI would require breach notification.

HHS is required under HITECH to conduct periodic audits of CEs and BAs to ensure HIPAA compliance. They may not audit you, but they might audit your client and you will need to have systems in place to provide them with periodic reports.

Technical & Security Concerns

According to HHS, information access management and access control are the most commonly violated provisions of the security rule. The HIPAA Security Rule is all about

data: data in motion, data at rest, data in use and data disposed. Certainly, in our industry, everyone must be concerned about data both in motion and at rest. Data in motion includes data moving through a network, including wireless transmission, whether by email or structured electronic interchange. Messages containing PHI sent by email and/or cell phones or pagers all involve routes that are open to interception and/or misdirection. Data at rest includes data in databases, file systems, flash drives, memory, backup storage, even your laptop. All these areas are vulnerable to breaches.

You need to be sure that operators working for you remotely are also covered when you address the concerns above. Do you have the proper access controls both in your office and at your remote locations? How do you ensure that a remote operator's child doesn't gain access to PHI about a friend or a teacher?

HHS urges that all PHI be encrypted. If you encrypt, are your encryption keys stored on a separate device from the data? If you don't have the ability to encrypt are your firewalls and access controls stringent enough to prevent incursions from unauthorized individuals? What about your storage and destruction policies – do they adequately protect PHI? Do you shred data storage disks? Do you wipe the drives clean or remove the hard drive when you dispose of an old computer? Do you shred printed materials containing PHI?

Penalties

HITECH requires mandatory penalties for violations of HIPAA that are due to "willful neglect." Civil penalties are based upon the level of intent and neglect. Violations determined to be without knowledge start at \$100 per violation to a maximum of \$25,000. Violations based on reasonable cause start at \$1,000 per violation to a maximum of \$100,000. Willful neglect violations start at \$50,000 to a maximum of \$1.5 million!

HITECH allows private right of action. You can also be sued or named as a party in a suit by an individual whose PHI has been disclosed. Such expensive legal action should be avoided by ensuring you have the proper BACs, insurance, training, data protection, policies and procedures in place to minimize your exposure!

Outsourcing Implications

If you have individuals outside of your physical office serving clients with PHI usage, you must extend your security compliance to them also. Many TAS operations have remote operations that access the business's computers over the Internet. You must have security measures in place to protect the unsecured PHI at both the central and all remote locations and in transit between.

TASs that outsource some of their calls involving PHI to other businesses must be sure that these businesses are also HIPAA/HITECH compliant. Overflow during busy periods, client sharing, outsourcing to different countries with less expensive workforces are all areas of potential risk which would be borne by you as the business associate of your covered entity client. You will need to have contracts in place with these entities that protect you from breach and PHI disclosure. Hosted solutions present the same problems. Your contracts must address the very real concerns of the HIPAA/HITECH Security and Privacy Rules.

In Conclusion

HIPAA/HITECH has arrived. You need to be sure you are ready for it. Your competition will be.

First – do a risk assessment of your operations. Determine if you use PHI when providing services for a client. If you do, identify and list all areas where there is a potential for PHI disclosure and rate these areas for their level of vulnerability. Then, develop a plan to respond to these areas with the proper security procedures.

Be sure that all your technology is adequate to the tasks at hand. Access controls, firewalls, encryption or data safety are paramount both in the main office and at your remote operations.

Create policies for every aspect of PHI use, and then the procedures to carry them out. Be sure that you have developed instruments for reporting breaches and potential disclosures back to your CE client. Look to ATSI for assistance with policy development.

Develop and conduct training programs. All members of your workforce need ongoing security training. Helpful tools are to have reminder posters in the work area, computer login screen reminders, and online training in security procedures. Check with ATSI for industry-specific assistance with these needs.

Update your Business Associate Contracts to include the required Security & Privacy Rule clauses. ATSI will have model contracts for your use. But always remember to avoid anything that would obligate you beyond the basic statutory requirements.

Review your insurance to be sure you are covered against the new exposures brought by HITECH. ATSI's industry-specific Errors & Omissions insurance program has been reviewed by experts to ensure you are properly reducing your liability exposure and risk.

Make sure you have all the proper protection in your vendor contracts to ensure you are in compliance with the new requirements. A breach that occurs at an overflow or hosted solution site is your responsibility – protect yourself with ATSI's sample contracts.

Finally, if you have any doubts or questions, contact ATSI's Government Relations HIPAA Subcommittee for information and guidance at www.atsi.org/hipaa.

Charlene Glorieux is the executive vice president for ATSI, which has done extensive work in guiding call centers in these new regulations. For more information, contact her at admin@atsi.org or visit www.atsi.org.

Definitions:

ARRA: American Recovery & Reinvestment Act (aka the Stimulus Bill)

BA (Business Associate): any entity that engages in health information exchanges or provides data transmission of PHI

BAC: Business Associate Contract

Breach: the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the PHI

CE (Covered Entity): health plans, health care clearing houses, or health care providers that transmit any health information electronically in connection with a covered transaction.

EHR: Electronic Health Record

EPHI: Electronic protected health information

HIPAA: Health Insurance Portability and Accountability Act

HITECH: Health Information Technology for Economic and Clinical Health Act

PHI (Protected Health Information): individually identifiable health information that is transmitted or maintained in any form or medium, including electronic information.
Unsecured PHI – protected health information that is not secured through the use of a technology or methodology specified by the HHS Secretary in guidance.