Transcription Compliance under HITECH

Save to myBoK

Joanne Glunt, senior VP of field operations at Webmedx, and Edna Palmer, manager of central transcription at Bon Secours in Richmond, VA, describe steps covered entities can take to mitigate privacy and security risks and keep compliant with the new regulations.

HITECH changes to the HIPAA privacy and security rules put new responsibilities on both providers who outsource medical transcription and the companies that provide services for them.

When President Obama signed the American Recovery and Reinvestment Act (ARRA) in February 2009, the HIPAA rules for privacy and security of protected health information (PHI) became more accountable, enforceable, and subject to litigation. A healthcare provider's responsibility for controlling protected health information (PHI) was greatly expanded—as were the penalties for failing to do so.

The changes have direct impact on the decisions a provider makes on medical transcription: where services will be performed, who will be performing them, and how the agreements will be written. There are new concerns to contemplate, new criteria to weigh, and new items to add to checklists.

Outsourcing under HITECH: What's New

HIM's ability to comply with HIPAA is easiest if medical transcription is performed in-house, under an organization's own internal policies and security procedures. However, this is not the norm. In most situations, medical transcriptionists (MTs) are working outside an organization's four walls and beyond HIM's immediate control. As the degrees of separation increase, so do the risks for breach of information.

Most MTs work from home, or other locations outside the facility. Coupled with at-home MTs, most provider organizations have a handful of independent contractors (ICs) to augment the internal workforce. Hence the first degree of separation and first layer of HIPAA risk.

In addition, many HIM directors outsource a portion of the transcription workload to a medical transcription service organization (MTSO) that performs the work in different parts of the United States. Last, and perhaps most open to risk, is outsourcing transcription to a MTSO that performs the work offshore. The more degrees of separation, the less control HIM directors have and the greater risk to CEs under HIPAA.

The modifications to HIPAA help provider organizations by making business associates (BAs) just as liable and contractually obligated to protect PHI as the provider. Both partners now are subject to the same civil and criminal penalties. Even subcontractors of BAs have the same responsibilities and potential fiduciary and legal downsides as every other party involved in processing PHI.

- Employees of covered entities as well as ICs and BAs are now subject to civil penalties and legal accountability.
- Health and Human Services (HHS) is legally bound to investigate all complaints.
- Civil penalties range from $100 to $50,000 and can be up to $100,000 to $250,000 with jail time if false premises or data selling are involved.
- All breaches of unencrypted PHI must be disclosed. Breaches of more than 500 records most be disclosed to the media.
- HHS is required to conduct periodic compliance audits.
- All BAs must have written policy and procedure manuals and must have performed a risk assessment.

Offshore Requires Greater Scrutiny

Compliance with the new provisions is greatly complicated when MTSOs are located offshore. This is because foreign countries are not bound by U.S. Law, and therefore HIPAA and HITECH have no standing. Even more daunting is the possibility that the offshore entity is using subcontractors. While HIM directors may have some recourse contractually with an offshore MTSO, it is doubtful they have any options with the vendor's subcontractors should a breach occur.

Covered entities within the United States must answer to U.S. law, regardless of where the breach occurs or how far removed the guilty party is from the covered entity. Hence, covered entities are wise to place greater scrutiny on their offshore transcription services now that new HIPAA rules are in force.

Devil in the Details: Technical, Legal, and Operational

In the end, there is no easy answer to ensuring that PHI is kept private. Laws, contracts, policies, and procedures are vital, but ultimately covered entities rely on individuals to do the right thing.

"The best course of action for HIM directors is one of solid due diligence," says Susan Lucci, RHIT, CMT, AHDI-F, 2010/2011 past-president of AHDI, the Association for Healthcare Documentation Integrity. "They can engage internal IT and legal resources to help make transcription outsourcing decisions. IT staff can ensure that data protection is in place, while legal counsel will assist with writing MTSO contractual obligations and delineating [covered entity] versus BA responsibilities."

From a technical perspective, data and voice files must be encrypted while being transferred and while at rest on a server. This practice makes it much more difficult for cyber-thieves to access PHI.

Second, the files should be stored on a U.S. – based server in a secure location. MTs should access the information they need, with appropriate security, perform the work on the U.S. server, and the MTSO or the covered entity's IT department should maintain control of the information. Information is much more secure if accessed on a virtual private network, or VPN, rather than over the Internet.

There must be complete audit trail accountability to ensure that PHI is accessed on a "need to know" basis. Finally, the CE should have a solid disaster recovery plan and test it regularly.

Legal counsel will help write and review the MTSO contract, which must include HIPAA protection clauses for vendors located outside the US. Indemnification, contractual penalties, and all transparency issues must be clearly stated and enforceable.

Many countries have their own privacy laws, which should be included in the MTSO's contract to ensure accountability. The more detailed the contract, the less opaque offshore transcription becomes.

Finally, MTSOs are business associates, and they must have a compliance or security officer to oversee the entire HIPAA process. Each business associate must conduct security risk assessments to identify potential areas of vulnerability. And they must have a notification policy and procedure in the event of a breach. Federal law specifies which breaches must be reported, what information is required, and who must be notified. Many states have their own notification laws, which may add additional requirements.

HIM Directors should carefully review each of the items mentioned above and discuss them in detail with transcription services partners, especially those performing work offshore. Agreements should be properly documented and reviewed. Keep in mind that HIPAA/HITECH issues are a small, albeit crucial part of any offshore outsourcing contract.

Key Questions to Ask

While HIM Directors may never be completely satisfied that PHI is being protected and offshore transcription services fully comply with HIPAA, these technical and legal steps work well to mitigate privacy and security risk.

Technical Questions

- Are data and voice files encrypted during transfer and at rest?

- Are files stored in a U.S.-based server and in a secure location?
- What is the disaster recovery plan? Is it tested regularly?
- Who controls the information?
- Is there an audit trail?
- Are files transported and accessed via VPN?

Legal Questions

- What remedies for indemnification exist?
- What are the contractual penalties for a breach?
- Where will work be performed and by whom? (Address transparency and subcontractor issues)
- Is accountability with U.S. privacy laws included?
- What is the breach notification plan?
- Are country-specific security and privacy laws included?

Operational Questions

- Are HIPAA policies and procedures in place? (Ask to review)
- How frequently are internal security audits (risk assessments) performed?
- What is the issue or problem escalation hierarchy?
- Is there a privacy and security officer in place?
- Who has access to PHI and for what purpose?
- What privacy and security training do MTs receive?

In a best case scenario, having strict HIPAA policies, procedures and contractual agreements in place will protect a covered entity from exposure. In the worst case, it demonstrates that the provider made a best-faith effort, and it may serve to remove criminal liability in case of a breach. Finally, if HIM Directors must go offshore for medical transcription services, risks will increase. The more transparent everything is throughout the service partnership, the safer providers will be.

Original source:
Glunt, Joanne; Palmer, Edna. "Transcription Compliance under HITECH" (Journal of AHIMA website), November 01, 2010.
