# Red Alert to HIPAA Business Associates—HITECH Is Here!

by Brenda J. Hurley, CMT, AHDI-F

The American Recovery and Reinvestment Act (ARRA) and its Title XIII called the HITECH (Health Information Technology for Economic and Clinical Health) Act greatly expand on HIPAA compliance requirements. HITECH has extended to business associates (i.e., MT services) the data privacy and security requirements that had been required previously by covered entities (clients). Business associates (BAs) will now be subject to civil and criminal penalties, including a provision that allows patients to receive financial compensation for a violation of their privacy.

Enforcement under this new federal law has new teeth. Here is a summary. The new law

- Clarifies that employees or other workforce members (independent contractors) are subject to civil penalties. So legal accountability has now been expanded to individuals.

- Requires HHS to formally investigate any complaints and impose civil penalties for violations of rules due to "willful" neglect.

- Requires that any civil monetary penalty or settlement amount as a result of a privacy or security rule violation be transferred to the Office for Civil Rights to be used for enforcement of the HIPAA privacy and security rules.

- Establishes a tiered system of civil monetary penalties ranging from $100 for unknowing violations up to $50,000 for each violation due to willful neglect. The Secretary of HHS determines the penalty amount for the violation.

- Requires the Secretary of HHS to conduct periodic audits to ensure covered entity and business associate compliance with new rules.

- Gives the State Attorneys General the authority to bring suit in district counts for any violation on behalf of state residents.

It is fair to say that the changes promulgated by HITECH have truly rocked the world of medical transcription businesses with new regulatory requirements and obligations. Just to be clear, medical transcription business associates include medical transcription businesses and MT independent contractors who work directly for a covered entity (doctors, clinics, imaging center, hospital, etc.). Here is a summary of some of the major changes now effective for MT business associates.

- **A designated security official is needed**. This is the go-to person for compliance issues and the individual who will quarterback the compliance activities for the organization. While corporate compliance is truly everyone's job, a coordinator is needed to make sure that the organization gets on track and stays there. This individual does not need to be an employee; it could be a consultant who fills this role. I often tell people that your security official is the person that HHS will ask for when they show up at your door for an audit. If you think that is funny, it is not. HHS is required under the law to do periodic audits of covered entities and business associates; included under their obligation to Congress is to publish those audit results in an annual report.

- **Encryption of all protected health information (PHI)—both during transmission and when in storage—is included under HITECH.** At least two states have already required encryption prior to this new federal law, so perhaps this is not a new practice within your MT business. Many have been using encryption with transmission, but encryption for stored data has not been quite as common. Now all data at rest (stored) or in motion (transmitted) are required to be encrypted to prevent a breach. HHS provides guidance for the protection of data and at this time it is 128-bit or 256-bit encryption. This guidance will be reviewed annually by HHS.

The guidelines for the protection and destruction of data are published by NIST (National Institute of Standards and Technology). These are free publications that can be found

***A designated security official is needed. This is the go-to person for compliance issues and the individual who will quarterback the compliance activities for the organization. While corporate compliance is truly everyone's job, a coordinator is needed to make sure that the organization gets on track and stays there.***

at **www.nist.gov**. The encryption and the appropriate destruction of PHI are critical processes for MT businesses to embrace because when PHI is "secured" through these processes a breach is avoided. Unsecured PHI is defined as not secured through the use of a technology or methodology that renders the PHI unusable, unreadable, or undecipherable to unauthorized individuals.

• **Breach notification obligations and responsibilities are now extended to the business associate.** HIPAA had already required business associates to provide covered entities (their clients) with a Report of Disclosure for inappropriate disclosure of their PHI and to keep a record of those disclosure reports for 6 years. So MT businesses should have already been doing this since the HIPAA privacy rule was enacted in 2003. The covered entity would then include this information in its files for when patients request an accounting of their disclosures (a right provided to patients under the original version of HIPAA).

A breach is defined as an "acquisition, access, use, or disclosure" of **unsecured** PHI that is not otherwise permitted under HIPAA "which compromises the security or privacy" of the PHI. As discussed above, *unsecured* means *unencrypted*.

Business associates are still required to notify the covered entity (their client) without unreasonable delay when there is a breach discovered. The covered entity will likely establish a timeframe for notification within the business associate agreement or amendment (more on that later) because the patient has to be notified of the breach no later than 60 days from the time of the breach discovery. State laws that permit less delay for patient notification preempt. So reporting to the client any breach discovery should be done without undue delay. If the breach involves more than 500 people, the major media outlets have to be notified. There are specific requirements for the manner and form of this notification, but most notable is that such notification is to be done by the covered entity **or the business associate** involved in the breach.

• **There is no requirement to execute totally new business associate agreements for clients who have current agreements in place.** An amendment can be crafted with language consistent with the new business associate requirements, then executed with those clients. The option does exist, however, to forego an amendment and instead execute all new business associate agreements for current as well as new clients. Both the covered entity and the business associate are equally obligated to update and execute an agreement or amendment that reflects these expanded requirements. Since most agreements are crafted to protect the party that created them, MT businesses should consider drafting a standard business associate agreement to present to their current and future clients in order to avoid language that might be included in an agreement provided by a client that would increase the business associate's legal burden.

• **It is now the legal obligation of the business associate (MT service) to take reasonable steps to try to stop any violations by its client (the covered entity).** If resolution does not occur, the business associate must report its client to HHS. This "policing" is the same for both parties—the covered entity and business associate are equally required by law to report violations by either party to HHS.

• **Business associates are now held accountable to all elements of the HIPAA Security and Privacy Rule**. While business associate agreements already have required adequate administrative, physical, and technical safeguards to be in place to protect the PHI received from their clients, most have not included additional specific privacy and/or security requirements. This expansion of obligations impacts MT businesses in many ways; one is the requirement for the business associate to have written documentation of a formal security risk. Given the large amount of data processed daily by medical transcription businesses, the importance of conducting and documenting a diligent security risk analysis process cannot be overstated. Some MT businesses may have already completed this since identifying potential gaps and risks related to data are critical to good security practices.

Under the Security Rule, another requirement is a **complete audit trail** for the access of all data (voice and text), actions performed, and by whom. Many MT businesses already have this in place because knowing this information and being able to track data activity equates to good business practices.

Yet another requirement under the Security Rule is **contingency planning**. HIPAA states that the purpose of a contingency plan is to have an established coordinated strategy that involves plans, procedures, and technical measures to enable the recovery of systems, operations, and data after a business disruption. The primary objective is to reduce the level of risk for loss or breach of data and to reduce the time for business disruption so that authorized individuals can have access to vital systems and information when required. It was because of the importance placed on this "availability" principle that the plans for data backup, emergency mode operations, emergency access procedures, and a disaster recovery are all required implementation specifications under the Security Rule, and now required of business associates.

A contingency plan encompasses the processes included in plans for data backup, emergency mode operation, emergency access procedures, contingency operations, and disaster recovery.

• **Security with a remote workforce is a challenge for MT businesses because HIPAA holds the business associates responsible for the actions of their workforce**. Training is required to educate their workforce members as to their obligations related to the privacy and security of PHI. Individually (each member of the workforce) and collectively (the MT business) can now be held legally responsible for their actions.

Think of security in three phases with each important to the organization. Phase 1 is **prevention**—know your risks through a security risk analysis and use appropriate methods for protecting the data and secure authentication for access. Phase 2 is **detection**—perform regular monitoring and auditing with documentation of these activities. Phase 3 is **response**—incident handling response process, breach notification processes, and disciplinary actions through sanctions.

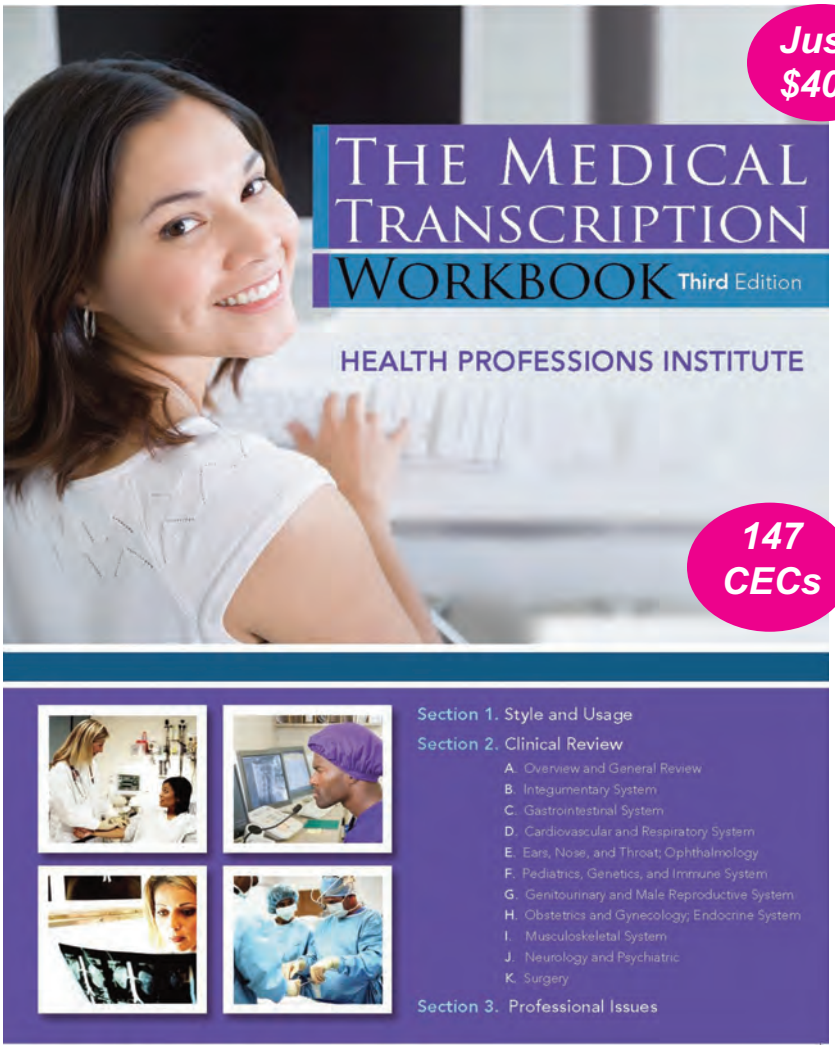
• **Formal written policies and procedures are needed for all of the items listed above and so much more**. Sanction policies are required for corrective action and steps for remediation when a breach occurs. Processes like termination of staff need to be formalized to eliminate their access to PHI so those individuals are completely removed from your systems in an intentional and timely manner in order to eliminate their access to PHI.

***HIPAA states that the purpose of a contingency plan is to have an established coordinated strategy that involves plans, procedures, and technical measures to enable the recovery of systems, operations, and data after a business disruption.***

Clearly the medical transcription industry has formidable challenges for compliance with these new HITECH requirements, not only because of the enormous amount of data that is handled, stored, and transmitted on a daily basis, but also because of the large number of remote workforce. For those reasons, some people call this HIPAA version 2; I call it *HIPAA on steroids*!

Brenda J. Hurley, CMT, AHDI-F, is a consultant in the medical transcription industry. She can be reached at **bjhurley@aol.com.**

**1 Medicolegal CE credit approved**




## Now arranged by medical specialty!

***The Medical Transcription Workbook***, 3rd ed., has been thoroughly reformatted to help students and transcriptionists identify, learn, and assess their knowledge of medicine and professional issues. This edition includes the following:

**Style and Usage** quick reference section, arranged alphabetically by topic, with hundreds of examples and exercise worksheets.

**Clinical Medicine** sections divided into major medical specialties or body systems. Previous sections in anatomy and physiology, medical terminology, pathophysiology, laboratory, and pharmacology are integrated within each medical specialty. Hundreds of worksheets with matching exercises, multiple choice, fill-in-the-blank, and true/false exercises are included in each section.

**Professional Issues** section with articles on the healthcare record, HIPAA and confidentiality, interpretation and editing of dictation, risk management, quality assurance, electronic resources, health in the workplace, and professionalism.

The readings and exercises also facilitate the preparation, taking, and passing of medical transcription employment and credentialing examinations. The new arrangement by medical specialty or body system is ideal for study groups and for supplementing textbooks in MT education programs.

## Answers to Exercises are on a CD at the back of the workbook.

### Buy the whole bundle of HPI workbooks for just $100. (Save $48.)

***H&P: A Nonphysician's Guide to the Medical History and Physical Examination***, 4th ed.
24 CECs $34.00

***Human Diseases, 2nd ed.***
20 CECs $36.00

***Laboratory Tests & Diagnostic Procedures in Medicine***
24 CECs $38.00

***The Medical Transcription Workbook***, 3rd ed.
147 CECs $40.00

**www.hpisum.com**


## Download sample chapters at www.hpisum.com.