HIPAA COMPLIANCE FOR MTSOs

HIPAA regulations affect our industry in many ways. The two main areas of impact are privacy and security. The privacy regulations address many areas with the most pertinent being electronic transactions, use and disclosure of protected health information, written policies and procedures, written business associate agreements and employee/staff training. The security regulations require administrative, physical and technical safeguards, as well as organizational requirements that cover the written policies and procedures, documentation, and risk analysis/management.

There are many forms of protected health information (PHI) that we must be cautious about circulating too freely. Security regulations through HIPAA require protection of those elements. Some examples are:

- Names
- Geographic subdivisions
- Dates, except year
- Birth date
- Phone #
- Fax #
- Email and/or web addresses
- Device identifiers
- SS #
- MRN
- Health plan #
- Account #
- DL #
- Vehicle serial #
- IP address
- Biometric identifiers
- Photographic images
- Other unique identifiers

As a medical transcription company you are considered a Business Associate (BA) which performs functions for Covered Entities (CEs) and work directly with them. According to the new HIPAA regulations you are held to the same regulations and laws as those covered entities. Medical transcriptionists fall under the classification of Business Associates.

Changes Effective on September 23, 2009, requiring compliance include the following:

- Notification Of Breach of unprotected personal data (unencrypted) to covered entities by business associates. (BA)
    - BAs notify CE of the data that has been breached
    - CE must notify the individual of the breach or CE can choose to have the BA contact the individual.
    - Patient is notified "without undue delay" but no later than 60 days; state laws may require faster notification.
    - CE notifies HHS in its annual report
    - If the breach involves more than 500 people, the "major" media outlets have to be notified and the HHS is immediately notified. i.e.: a technical glitch allowed an unencrypted stream of PHI
    - BAs are also subject to civil and criminal penalties.
    - State privacy laws would also apply both in action taken and in penalties; including a provision that allows individuals to seek financial compensation for damages for a violation of their information.
    - Example: Copies of a report are requested to be sent to Dr. David Smith per the dictating doctor; out of the multiple Dr. David Smiths, the MT inadvertently chooses the incorrect one. The PHI is sent to the wrong doctor. The following steps must take place:
        - Notify the BA
        - Notify HHS
        - Write a report
        - Make an accounting of disclosures for the patient's records

        - Notify the patient/individual of the breach. “You’re report was faxed to the wrong Dr. David Smith.”
- Must do a Risk Analysis to check for possible breaches.

- What is a Breach?
    - Unencrypted is Unprotected!
        - Any CE or BA that “accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses or discloses” unsecured PHI must notify individuals whose unsecured PHI has been (or is reasonably believed to have been) accessed, acquired, or disclosed as a result of a breach.
        - “Unsecured” PHI means PHI that is not secured per HHS guidance (which will be issued annually)
    - Harm Threshold
        - Poses a significant risk of financial, reputational, or other harm to the individual.
    - ADA guidelines
        - Notification must accommodate those with disabilities. i.e.: blind patients.
    - Not Reportable if it is an….
        - Unintentional access by a member of the workforce acting under authority of a CE or BA, thus it is forgivable provided the PHI was reviewed in good faith, under the workforce umbrella and was not further disclosed.
            - i.e.: MT picked the wrong patient – clicked on them and then got out and chose the correct patient.
    - Reportable if it is….
        - Unprotected personal data in any media (paper, CDs, computer hard drive, email, etc.)
        - Electronic media must be cleared, purged, or destroyed according to the guidelines in the NIST publication on Guidelines for Media Sanitization.
        - Delivery methods, addresses, fax numbers and other information should be kept current or be removed from address books.
            - i.e.: Dr. David Smith moved and the fax # is now a gas station. The level of significant risk is a full breach.

- Sanction Policies for Breaches
    - CEs and BAs need to develop written sanction policies for corrective, active, and remediation steps if a breach occurs.
    - Sanctions may be adjusted depending on the following:
        - Multiple offenses
        - Harm to the breach victim(s)
        - Breach of specially protected information such as HIV-related, psychiatric, substance abuse, and genetic data.
        - High volume of people or data affected.
        - High exposure for the organization.
        - Large organization expense incurred, such as breach notifications
        - Hampering of the investigation
        - Negative influence of actions on others
        - Victim(s) suffered no harm
        - Offender voluntarily admitted the breach and cooperated with the investigation
        - Offender showed remorse
        - Action was taken under pressure from an individual in a position of authority
        - Employee was inadequately trained.

- Breach Sanction Categories
  - Category 1: Unintentional breach of privacy or security that may be caused by carelessness, lack of knowledge, or lack of judgement, such as a registration error that causes a patient billing statement to be mailed to the wrong guarantor.
  - Category 2a: Deliberate unauthorized access to PHI without PHI disclosure.
    - Example: snoopers accessing confidential information of a VIP, coworker, relative, or neighbor without legitimate business reason;
    - Example: failure to follow policy without legitimate reason, such as password sharing.
  - Category 2b: Deliberate unauthorized disclosure of PHI or deliberate tampering with data without malice or personal gain.
    - Example: snooper access and re-disclosure to the news media
    - Example: unauthorized modification of an electronic document to expedite a process.
  - Category 3: Deliberate unauthorized disclosure of the PHI for malice or personal gain.
    - Example: selling information to the tabloids
    - Example: stealing individually identifiable health information to open credit card accounts.

Changes that are effective February 17, 2010 cover even more liability for BAs. They include the following:

- Employees or other staff (contractors) who work for BAs or CEs will be individually subject to civil penalties.
- BAs are required to have a formal compliance program (training) with sanctions for their workforce.
- BAs will need to have a complete audit trail for access of the data.
  - Audit Trail = the chronological set of records that provides evidence of information system activity. Data are collected about every system event (log-in, log-out, file access, etc.) and used to facilitate the determination of security violations.
  - For MTs:
    - Your system activity will be tracked by the audit trail system.
      - Log-in
      - Access
      - Time spent
      - Actions performed
    - These activities can be matched to the actions needed to perform your duties.
    - Remember it is NOT a reportable breach if:
      - It is unintentional access by a member of the workforce acting under authority of a CE or BA, thus it is forgivable provided the PHI was reviewed in good faith, under the workforce umbrella, and was not further disclosed.
      - Audit trails can provide the proof needed to confirm that a breach was unintentional… or not!
    - Remember you are not allowed to use or disclose PHI for any purpose beyond the scope of your duties. This purpose is defined within the BA agreement.
    - The audit trail will be the proof needed to verify that you acted appropriately within the scope of your duties… or the evidence needed to prove that you did not.

- BAs are subject to periodic audits by HHS.
    - Targeted sooner to make sure BAs are on track
    - There is specific money budgeted for these audits and all money from fines stay in the department to add to the auditing resources.
- BAs are required to appoint a security official.
- All stored and transmitted data will need to be encrypted -- some states already require this.
- New BA agreements will need to be crafted with these changes and executed between the MT service and the CE.
    - An amendment can be used for current clients when BA agreements are already in place.
- BAs will be required to conduct a thorough security rick analysis. This documentation must be available for investigators if audited.
- BAs will need administrative and technical safeguards established, implemented, and written Policy & Procedures for each.
- If the BA finds that the CE is violating the federal privacy/security rules, the BA is obligated under the law to…
    - Try to get the CE to "cure" the violation and if that does not occur…
    - If "cure" does not occur, report the CE to HHS.
    - Termination of the contract is also an option.
    - NOTE: The CE has this same responsibility (and steps to follow) if it is the BA that is violating the law.
    - The "doctor" can't take away your responsibilities with the law. No more "it's on me" stuff.

SECURITY RISK ANAYLSIS: (things to include)

- Controlling access:
    - Sanctions
    - Workforce compliance
    - Workforce security
        - Making sure the person on the system is the person they say they are. (India?)
    - Termination process
        - Taken out of the system: HR & IT
    - Access authorization
    - Log-in monitoring
    - Password management
        - Changes periodically
    - Periodic evaluation
- Physical Safeguards
    - Facility – remote workplace security
    - Workstations – others use PC?
    - Device Media Controls – any personal data needs to be encrypted
    - Accountability
- Technical Safeguards
    - Unique user ID
    - Automatic logoff
    - Audit control
    - Use of authentication tools
    - Data storage with encryption
    - Transmission security with encryption

New Laws Bring New Risks to MTs and MT Companies

- Any PHI on your PC will need to be encrypted both at rest (stored) and in motion (transmitted)
- Be alert to avoid breaches
    - Copies of reports
    - Faxes
        - not encrypted, so it is a breach if it is sent to the wrong place
        - if it comes from your system you are liable regardless of who "sent" it.
        - Sending control of faxing back to the CE is the best way to avoid liability for misdirected faxes.
    - Emails
- Training for the workforce is required
- There is a new tiered system of civil monetary penalties based on the category of the violation.
- Patients can sue MT companies and/or individuals for damages using HIPAA as the standard for care of their PHI.
- Be Alert to Risks
    - De-identify reports whenever possible (i.e. sample reports, reports used for the QA process)
    - Protect backup media from unauthorized access through physical security measures and encryption
    - Do not keep PHI (even audio) stored any longer than necessary to minimize risks for a potential breach. Do it now!
        - Minimum of 6 months/1 year
        - Provide data on CD to CE if needed.
    - Implement tight security within your (home) office.
        - Restrict others from using your PC
        - Protect materials with PHI from viewing and accessing by others.
        - DO NOT PARTICIPATE in unsafe security practices.
    - Use the HIPAA notice of confidentiality on the fax coversheet when fax is necessary.
    - Shred all paper that contains any PHI. Do not put any paper with PHI in trash bins.
    - Do not leave any materials with PHI in unattended areas where unauthorized individuals may have access to it.
    - Locate printers and fax machines in a secured area away from access by others.
    - Abide by established Policy &Procedures that protect privacy and security of PHI
    - Do not disclose PHI for any purpose beyond the scope of your current responsibilities.
    - Report to your supervisor (or client) when dictation is performed in a public location.
        - This practice could be a breach – so it needs to be reported.
    - Be proactive for ways to prevent potential breaches.

OVERVIEW OF SPECIAL CHALLENGES FOR THE MT INDUSTRY:

- Large amounts of data generated, transmitted, and stored
    - Data centers
        - Access and security practices
    - Report distribution to multiple locations (Must be secure but is subject to breach notification)
        - Fax
        - Auto-faxing
        - Remote printing
        - Email (internal and external)—better with encrypted attachments and use only job #s and no patient information if possible.
        - Electronic transmission

(Going back to clients handling the distribution of reports will result in less liability)

        - Laptops and other portable media
            - Should have encryption software
            - Theft and security practices
        - Off-site storage
            - Access and security practices
    - Network
        - Remote accesses for workforce
            - Security practices—identify and authenticate; password or double encryption
            - Fingerprint scans a possibility
        - Remote accesses for clients (status reports, retrieving reports)
            - Security practices—passwords; appropriate clearances
- Home-based (remote) workforce
    - Employees
        - Training and proof of it
        - Security practices
        - PHI on their PC
            - Delete by end of day all PHI
            - Delete after use
        - Access to their PC
            - Restricted to MTs only is suggested
            - Usage restrictions outlined
            - Some companies provide the PCs for more control.
        - Email communications
    - Contractors
        - Training and proof of it
        - Security practices
        - PHI on their PC
        - Access to their PC
        - Email communications
- Key Driving Factors for Documentation Compliance
    - Legal risks related to fraud and malpractice, and the penalties associated with them.
    - Proof of services for appropriate (optimal) reimbursement. (CEs)

The Red Flags Rule is a federal law created to protect consumers from identity theft and medical identity theft. It will become effective on June 1, 2010 and will be enforced by the FTC (Federal Trade Commission). These rules will also potentially affect BAs as well as CEs. Some things to be aware of involving the Rule are as follows:

- Red Flags Rule requires:
    - Staff training including healthcare providers
    - Routine monitoring for people accessing patient files and noting any suspicious activity in patient accounts
    - Formal risk assessment
    - Written Policies &Procedures
    - Regular review of the program to assess its effectiveness
    - Documented proof of the program's implementation and administration
- What does this mean to MTs and MT Companies?
    - Limit the type of patient data received from CEs to only what is needed to perform the duties described within the BA agreement.
        - For example: never accept credit card information from the CE

        - Depending on the client requirements for patient demographics consider restricting other items.
            - Social security number
            - Address
            - Driver's license number
            - Other unnecessary unique identifiers
        - Can and probably should restrict the information that is in the MT distribution
        - No patient addresses unless it is required in a letter.
- Organizations can be penalized as high as $2,500 for each Red Flags Rule violation.

TERMINOLOGY:

- HIPAA –Health Insurance Portability and accountability Act
- PHI – Protected health information (information in any form or medium that is individually identifiable)
- CE (Covered Entity) – healthcare provider or facility, insurance plan, HMO
- BA (Business Associate) – Business or Individual who works directly with and performs functions for a CE
- ARRA – American Recovery and Reinvestment Act, aka The Stimulus Plan
- HITECH – Health Information Technology for Economic and Clinical Health (title XIII of ARRA)
- HHS – Health and Human Services
- OCR – Office of Civil Rights
- AHIMA – American Health Information Management Association
- POA – Present on Admission
- RAC – Recovery Audit Contractors
- E/M – Evaluation and Management
- CMS – Centers for Medicare and Medicaid Services

References:
Brenda J. Hurley, CMT, AHDI-F, ROSe Introductory Compliance Class
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Information Technology For Economic And Clinical Health Act (Hitech)