HIPAA COMPLIANCE
for
MEDICAL TRANSCRIPTIONISTS

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

HIPAA REGULATIONS:

Privacy involves:

- Electronic transactions
- Code sets
- National identifiers
- Use and disclosure
- Written Policies &Procedures
- Written BA agreements
- Training

Security:

- Safeguards
  - Administrative
  - Physical
  - Technical

PROTECTED HEALTH INFORMATION:

- Privacy regulations define PHI as individually identifiable health information transmitted or maintained in any form or medium – this includes dictations.
- The Security Regulations extend this to electronic protected health information (ePHI) as well.
- Identifiable elements:

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

- Covered Entities are Healthcare Providers, Health Plans, or Healthcare Clearinghouses.

- Business Associates (Company or Individual) perform functions for CEs and work directly with them. They must have a written Business Associate agreement. Use and disclosure of PHI must be only as agreed per contract and per HIPAA regs. <u>MTs fall under this as well.</u>

CHANGES EFFECTIVE ON SEPTEMBER 23, 2009:

- What is a Breach?
  - Unprotected is Unencrypted!

        - 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.
    - 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.
            - ie: 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.
            - ie: 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
    - ***List our sanction policies here***
    -
    -
    -
    - ….
    - 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 redisclosure 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 EFFECTIVE FEBRUARY 17, 2010

- Employees or other staff (contractors) who work for BAs or CEs will be individually subject to civil penalties.
- *Formal compliance program (training)* with sanctions for their workforce.
- A complete audit trail for access of the data will be in place.

- 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.

- 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.

New Laws Bring New Risks to MTs

- Any PHI on your PC will need to be encrypted both at rest (stored) and in motion (transmitted)
- Training on compliance is required
- Patients can sue MT companies and/or individuals (MTs) 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.
    - Delete by end of day all PHI
    - Delete after use
  - 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.
  - 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 P&Ps 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 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.

NEW PENALITIES ARE COSTLY

- BAs can be fined $100 to $50,000 (and more) per violation with a tiered system that could go to a total of $1.5 million per year.
- Individuals and BAs are subject to civil and/or criminal penalties.
- Individuals and BAs can be also held accountable to state courts for violating these rules on behalf of state residents.