HIPAA Privacy and BAA

Health Insurance Portability and Accountability Act (HIPAA)

- Creates national standards to protect individuals' medical records and other personal health information.

Who must comply?

- Covered Entities (CE):
  - Health care provider, health plans.
- Business Associates (BA):
  - Person who, on behalf of a CE, performs or assists with an activity involving the use or disclosure of individually identifiable health information.
  - BA has a direct relationship with the CE.
- Subcontractors:
  - Same as a BA except it's an indirect relationship with the plan.
  - Example of functions: Claims processing, billing, legal, consulting, data aggregation.

Privacy Standards and Security Standards

- Apply to individuals' individually identifiable health information or protected health information (PHI).
- Restricts how CEs use and disclose PHI.

What is PHI? Information that relates to:

- Person's past, present or future physical or mental health.
- Provision of health care to a person; or
- Past, present or future payment for a person's health care.
- Must identify the individual or must be a reasonable basis to believe an individual can be identified using the information.
- Can be oral, written or electronic.
- Information is not PHI if it is de-identified.
  - Certain identifiers are removed, such as names, dates, telephone numbers, email addresses, SSNs, medical record #s, etc.

If it's not PHI, the Privacy/Security Standards do not apply.

- Can't have actual knowledge that the information could be used alone or in combination with other information to identify an individual.

When should you disclose PHI?

- Required if individual requests access to their own PHI or an accounting of PHI disclosures.
- Required to HHS to determine if the CE is in compliance with the Privacy Standards.
- Permitted to the individual who is the subject of the PHI.
- Permitted for treatment, payment or health care operations (only provide minimum necessary).
  - Treatment: provision of health care services by a provider.
  - Payment: determination of eligibility, coverage, COB, cost-sharing, adjudication of claims, billing and collection.
  - Health Care Operations: underwriting, risk rating and disease management.
- Permitted if a valid authorization (only provide minimum necessary).

When do you need a BAA?

- Between CE and BAAs (e.g., between plans and brokers).
- Between BAAs and Subcontractors (e.g., between brokers and general agents).
- Templates can be found at Dept of HHS website or ask Compliance Department.

How to be Compliant

- Prior to disclosing PHI verify identity of person.
- Limit use and disclosure of PHI to minimum amount of info for the purposes of the use or disclosure.
- Maintain all PHI in locked cabinet or room (office).
- Do not leave PHI on desktops or around workstation (home offices and rest of house).
- Use screensaver with password on computer.
- Turn off computer when leave desk.
- Shield computer monitors from view.
- Shred any discarded PHI.
- During telephone calls, limit use of names, medical diagnosis, etc. and no voicemails with information.
- All emails with PHI should have disclaimer.

What if there's a Breach?

- First step is to recall message (if sent by email).
  - If successfully recalled, the system will advise if the recipient opened the email. If not opened, no further action is necessary.
  - If not recalled or already opened or sent by other means than email, contact recipient immediately and tell them information was sent in error.
  - Destroy the information.
  - Do not forward or further disclose the information.
  - Send back written confirmation of destruction.
- Notify your manager right away.
- Managers must notify the Compliance Dept. with details as soon as possible.