

HIPAA is a critical topic for individuals and your organization - and it requires more than technology issues. Personal accountability is more complicated than database or email passwords. Handling individual health records with care requires a strong moral compass and a firm idea of what type of conduct violates HIPAA and puts your organization at risk. Keep this guide as a handy reminder of risky record keeping practices.

### COMMON VIOLATIONS:



- Failing to make reasonable efforts to ensure that any remote use or access to e-PHI is authorized and legitimate
- Discussing patient information in a public place or with unauthorized people
- Leaving print or electronic media where unauthorized people can read it
- Accessing records without a job-related need-to-know
- Sending PHI to the wrong place
- Failing to encrypt PHI or establish basic password protections
- Failing to train employees or consistently discipline HIPAA violators

### COMMON SENSE PRECAUTIONS:



- Position your computer screen so that PHI can't be seen by others in your office who don't have a legitimate business need to see it.
- Keep hard copies of PHI in a locked drawer before you leave your workspace—and keep the key with you.
- Don't discard PHI in regular wastebaskets.
- Lock your computer screen when you leave your desk.
- Don't share your passwords with others.
- If you are required or permitted to take PHI out of the office on a laptop or thumb-drive, take extra care to safeguard the PHI and encrypt it.
- Do not leave devices or media containing PHI in unattended cars or public areas.
- Avoid sending PHI by email unless the email is password protected and encrypted.