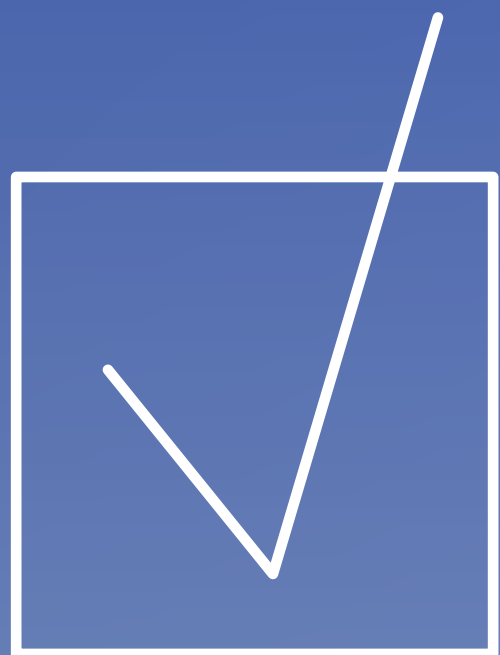


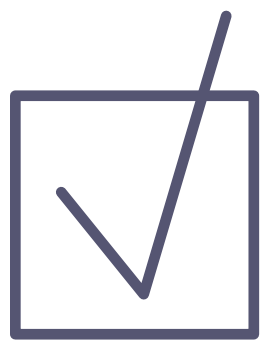


**emtrain**<sup>®</sup>

Checklist

# HIPAA Violations Risk Checklist





## Common HIPAA Violation Risks

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule governs how protected health information is created, accessed, stored, and transmitted. A firm understanding and adherence to HIPAA is crucial to both employers and employees. HIPAA violations can disrupt workflow and lead to expensive investigations and lawsuits. Handling personal health information (PHI) requires a strong moral compass and a firm understanding of what conduct violates HIPAA. Use this guide to help safeguard HIPAA-protected information.

### Common Violations:



- Failure to thoroughly ensure that any remote use or access to electronic PHI (e-PHI) is authorized and legitimate
- Discussing patient information in public or with unauthorized people
- Leaving print or electronic media where unauthorized people can see it
- Accessing records when it is unwarranted or superfluous
- Sending PHI to the wrong place
- Failing to encrypt PHI or establish basic password protections
- Failing to train employees on HIPAA or consistently discipline HIPAA violators
- Failing to lock your computer screen upon leaving your workstation

### HIPAA Best Practices:



- Position computer screens so PHI can't be seen by individuals without a legitimate business need to see it
- Keep all hard copies of PHI in a secure, locked location before leaving the workspace—and keep the key on hand
- Don't discard PHI in regular wastebaskets
- Use complex, secure passwords that include numbers, special characters, and uppercase letters
- When required or permitted to take PHI out of the office on a laptop or thumb-drive, take extra care to safeguard and encrypt the PHI
- Do not leave devices or media containing PHI in unattended cars or public spaces
- Avoid sending PHI by email unless the email is password protected and encrypted