Administrative, Physical, and Technical Safeguard Standards Compliance Worksheet

Administrative Safeguards
1. Security management process. A covered entity ("CE") must implement policies and procedures ("P&Ps") to prevent, detect, punish, and correct security violations.

   a. How is PHI transformed into EPHI within my practice?
   b. Who transforms PHI into EPHI within my practice?
   c. How is EPHI stored within my practice?
   d. Where is EPHI stored within my practice?
   e. Who has access to EPHI within my practice?
   f. What threats **reasonably** exist to the confidentiality, integrity, and availability of EPHI maintained by my practice? Computer hackers? Theft of EPHI or computer equipment by employees or outsiders? Unauthorized uses or disclosures by employees? Fire? Flood? Loss of EPHI because of computer system failure? Etc.
   g. For each threat to the confidentiality, integrity, or availability of EPHI identified in f. above, what can I do, given my technical capabilities and my financial resources, to prevent such threat from occurring or to detect security violations after they have occurred? Firewalls? Anti-virus Software? Etc.
   h. If I have an employee who commits a security violation, what kind of discipline will be meted out? Written warning? Notice of disciplinary action placed in personnel file? Removal of computer system privileges? Termination of employment? Etc.
   i. What can I do, given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, to monitor computer system activity? Tracking Log-ins? File Accesses? Security Incidents? Etc.

2. Assigned security responsibility. A CE must designate a person responsible for developing and implementing the CE’s security P&Ps.

   a. The person responsible for developing and implementing my security policies and practices is:

3. Workforce security. A CE must implement P&Ps to ensure that its employees have appropriate access to EPHI.

   a. If I do not have employees, then this section is not applicable to me.
   b. If I have employees, do all employees need to have equal access to all EPHI so that they can perform their work activities? Or, should access to EPHI for some employees be limited because they do not need access to all EPHI to perform their work activities? Should some employees not have any access to EPHI because they can perform their work activities without needing to access EPHI?
   c. As applicable, given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to limit the access of certain of my employees to EPHI?
   d. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to monitor my employees' use of their computers to determine that they are using and disclosing EPHI according to my security policies and procedures?
   e. When an employee leaves my employment, what can I do, given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, to prevent my former employee from accessing EPHI? Turning in office keys? Changing locks? Removal from access lists? Removal from user accounts? Etc.

4. Information access management. A CE must implement P&Ps for authorizing access to EPHI.
a. If I do not have employees, then this section is not applicable to me.

b. If access to EPHI is going to be limited for some employees, what can I do, given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, to limit such access? Granting or limiting access to systems, workstations, files, applications, records, fields, etc.?

c. If access to EPHI is going to be denied to some employees, what can I do, given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, to deny such access?

5. Security awareness and training. A CE must implement a security awareness and training program for its workforce.

a. If I do not have employees, then this section is not applicable to me.

b. What do I do now to train employees about my practice’s security policies and procedures, including, but not limited to, the appropriate use of passwords? Do they need additional training?

c. What will I do in the future to apprise my employees about changes in my security policies and procedures?

d. Have I apprised employees that they are not allowed to add any programs or applications to my practice’s computer system without my written permission?

e. Have I apprised my employees that they are not allowed to download any computer games, data, or software without my written permission? f. Do I have virus protection software in place to help detect malicious computer viruses? How will you keep such software current?

f. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to limit the number of log-in attempts to computers with access to EPHI?

g. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to create, change, and safeguard passwords?


a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to identify known or suspected security incidents?

b. Have I documented my policies & procedures for identifying security incidents?

c. Have I documented my policies & procedures for employees, as applicable, to report known or suspected security incidents to me?

d. Have I documented my policies & procedures for responding to known or suspected security incidents?

7. Contingency plan. A CE must implement P&Ps for responding to an emergency or other occurrence that damages the CE’s equipment or systems containing EPHI.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to backup my EPHI?

b. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, where and how will the EPHI that I backup be stored?

c. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, how can I recover EPHI if there is a fire, a flood, vandalism, or computer system failure?

d. Given some sort of natural disaster or other type of loss of EPHI, what EPHI is so critical to my practice, if any, that it must be restored first?
e. How often will I update my contingency plan?

8. **Evaluation.** A CE must perform a periodic technical and nontechnical evaluation to determine the extent to which the entity’s security P&Ps meet the requirements of the security regulations.

a. How often will I review my administrative, physical, and technical safeguards to determine whether what I am doing are reasonable and appropriate measures for maintaining the confidentiality, integrity, and availability of the EPHI that I create, receive, maintain, or transmit?


9. **Business associate contracts & other arrangements.** A CE must get satisfactory assurances from its business associates who create, receive, maintain, or transmit the entity’s EPHI or PHI that the business associate will care for the EPHI or PHI appropriately.

a. Do I have written business associate agreements on file in which my business associates agree to appropriately care for the EPHI or PHI they create, receive, maintain, or transmit?

**Physical Safeguards**

1. **Facility access controls.** A CE must implement P&Ps that limit physical access to electronic information systems and their locations to authorized individuals only.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, how can I limit access to my practice’s computers? Locks on doors? Alarms? Locating workforce members in positions within the office where they can see and control what is going on?

**Technical Safeguards**

1. **Access control.** A CE must implement P&Ps to limit access to electronic information systems that contain EPHI only to persons or software programs with access rights.

a. Do I have a password of at least 8 alphanumeric characters on my computer?

b. If I have employees, has each employee been assigned or does each employee have a password of at least 8 alphanumeric characters?

c. Are all of the computers in my practice equipped with an automatic log-off function so that casual observers cannot view computer screens?

3. **Workstation security.** A CE must implement physical safeguards for workstations that can access EPHI to protect them from unauthorized users.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to control physical access to my computers? Passwords? Automatic log-offs? Etc.

4. **Device & media controls.** A CE must implement P&Ps governing the transport (receipt & removal) of hardware and electronic media that contain EPHI into, out of, and within the organization.

a. What computer equipment and software is currently being utilized in my practice?

b. How will I dispose of old computers or computer equipment?

c. If applicable, have I informed my employees about my security policies and procedures regarding the disposal of old computers or computer equipment?

d. How will I cleanse storage media, such as diskettes, CDs, and DVDs, of EPHI before such media are reused?

e. If applicable, have I informed my employees about my security policies and procedures regarding the cleansing of storage media of EPHI?

f. Will I backup EPHI before any computers or computer equipment is moved?
so that such computers will automatically turn off after a predetermined period of time?

d. If the answer to c. above is no, given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to equip my computers with an automatic log-off function?

e. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do, if anything, to encrypt and decrypt EPHI?

f. If I am not going to encrypt EPHI before transmitting it over the Internet, have I informed my patients that transmitting such information may not be secure and that their confidentiality may be breached? Have I obtained written acknowledgement from my patients that they are aware of these potential problems?

2. Audit controls. A CE must install hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, how will I monitor system activity on my computers to determine that EPHI is being used and disclosed for authorized purposes only? Monitoring log-ins and log-offs? File accesses? File updates? File edits? Etc.

b. How often will I monitor system activity on my computers

c. to determine that EPHI is being used and disclosed for authorized purposes only?

3. Integrity. A CE must implement P&Ps to protect EPHI from being improperly changed or destroyed.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to ensure that EPHI is not altered without my knowledge or approval? Keep in mind, however, that if the CE is not hooked up to the Internet and if it has adequate access controls, then data authentication may not be necessary.

4. Person or entity authentication. A CE must implement P&Ps to ensure that persons or organizations seeking access to EPHI are who they claim to be.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, can I do to “authenticate” my employees or other third parties so that they can use my computers? Log-on passwords? Audit trails? Etc.

5. Transmission security. A CE must implement security measures to prevent unauthorized access to EPHI that is being transmitted over an electronic communications network.

a. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to ensure that EPHI is transmitted only to intended individuals or entities? Confirm e-mail addresses before sending? Etc.

b. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, what can I do to audit changes to EPHI to determine that such changes are legitimate and have been made by authorized individuals?

c. Given my technical capabilities, my technical infrastructure, my financial resources, and my desire to minimize to an acceptable level the risk of unauthorized uses or disclosures of EPHI, is encrypting EPHI a reasonable and appropriate safeguard for me to adopt?

Organizational & Documentation Requirements

1. Business associate contracts. A CE must ensure that its contracts or other arrangements (i.e., memorandum of understanding or agreement) with the CE’s business associates are amended to address the security regulations.

a. Do I have copies of my business associate agreements?
2. **Policies and procedures.** A CE must adopt P&Ps as reasonable and appropriate for the entity to meet the standards, implementation specifications, and other requirements of the security regulations.

   a. Have I adopted security policies and procedures that are reasonable and appropriate for my practice?

3. **Documentation.** A CE must maintain in written or electronic form the P&Ps that it has implemented to comply with the security standards. It must also document in written or electronic form any action, activity, or assessment that is required by the security regulations.

   a. Have I documented in writing my security policies and procedures?