d.

SECURITY STANDARDS CHECKLIST

"Required" = practice must take action to implement
"Addressable" = practice may not need to take action to implement

Administrative Safeguards

STANDARDS	IMPLEMENTATION SPECIFICATIONS	(R) =REQUIRED (A) =ADDRESSABLE	POL #	ALREADY IN PLACE	CUSTOMIZE P&P	NOT IMPLEMENTING	TRAINING COMPLETE
Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations *[Section 164.308(a)(1)]*	▪ **Risk Analysis** – conduct assessment of potential risks and vulnerabilities to confidentiality, integrity, and availability of electronic PHI (ePHI)	(R)	2	✓			
	▪ **Risk Management** – implement security measures to reduce risks and vulnerabilities	(R)	2	✓			
	▪ **Sanction Policy** – apply sanctions against staff who fail to comply with policies and procedures	(R)	2	✓			✓
	▪ **Information System Activity Review** – procedures to review records of information system activity	(R)	2	✓			✓
Assigned Security Responsibility: Identify a security officer *[Section 164.308(a)(2)]*		(R)	3	✓			
Workforce Security: Implement policies and procedures to ensure that staff have appropriate access to ePHI and prevent others from obtaining access *[Section 164.308(a)(3)]*	▪ **Authorization and/or Supervision** – procedures for authorization and/or supervision of staff who work with ePHI	(A)	4	✓			✓
	▪ **Workforce Clearance Procedure** – procedures to ensure staff access to ePHI is appropriate	(A)	4	✓			✓
	▪ **Termination Procedures** – procedures for terminating staff access to ePHI when employment ends	(A)	4	✓			✓

STANDARDS	IMPLEMENTATION SPECIFICATIONS	(R) =REQUIRED (A) =ADDRESSABLE	POL #	ALREADY IN PLACE	CUSTOMIZE P&P	NOT IMPLEMENTING	TRAINING COMPLETE
Information Access Management: Implement policies and procedures for authorizing access to ePHI *[Section 164.308(a)(4)]*	▪ **Isolating Health Care Clearing-house Function** – *not applicable to medical practices*	(R)	N/A				
	▪ **Access Authorization** – policies and procedures for granting access to ePHI	(A)	5	✓			✓
	▪ **Access Establishment and Modification** – policies and procedures for establishing, documenting, reviewing, and modifying users' right of access	(A)	5	✓			✓
Security Awareness and Training: Implement security awareness and training program for all staff *[Section 164.308(a)(5)]*	▪ **Security Reminders** – remind/update staff periodically regarding their security responsibilities	(A)	6	✓			✓
	▪ **Protection from Malicious Software** – implementation of policies and procedures to detect, report, and guard against malicious software	(A)	6	✓			✓
	▪ **Login Monitoring** – procedures for monitoring login attempts and reporting discrepancies	(A)	6	✓			✓
	▪ **Password Management** – procedures for the creation, changing, and safeguarding of passwords	(A)	6	✓			✓
Security Incident Procedures: Implement policies and procedures to address security incidents *[Section 164.308(a)(6)]*	▪ **Response and Reporting** – identify and document security incidents, response to such incidents, and the outcome of the incidents	(R)	7	✓			✓

Standards	Implementation Specifications	(R) =Required (A) =Addressable	Pol #	Already in Place	Customize P&P	Not Implementing	Training Complete
Contingency Plan: Implement policies and procedures defining how the practice will respond to emergencies or occurrences that could damage its ePHI *[Section 164.308(a)(7)]*	▪ **Data Backup Plan** – procedures to create and maintain exact copies of ePHI	(R)	8	✓			✓
	▪ **Disaster Recovery Plan** – procedures to restore any loss of data	(R)	8	✓			✓
	▪ **Emergency Mode Operation Plan** – procedures allowing the practice to continue doing business and continue to protect security of ePHI while operating in emergency/crisis mode	(R)	8	✓			✓
	▪ **Testing and Revision Procedure** – procedures for periodic testing and revision of contingency plans	(A)	8	✓			
	▪ **Applications and Data Criticality Analysis** – assess the practice's data and applications to determine which would be considered "critical"	(A)	8	✓			
Evaluation: Periodically evaluate technical and non-technical security safeguards to ensure compliance with Security Rule *[Section 164.308(a)(8)]*		(R)	9	✓			✓
Business Associate Contracts and Other Arrangement: Requires practices to enter into agreements with its "business associates" to ensure they will appropriately safeguard ePHI *[Section 164.308(b)(1)]*	▪ **Written Contract or Other Arrangement** – document the assurances required through a written contract or other arrangement with business associates	(R)	10	✓			✓

Physical Safeguards

Standards	Implementation Specifications	(R) =Required (A) =Addressable	Pol #	Already in Place	Customize P&P	Not Implementing	Training Complete
Facility Access Controls: Implement policies and procedures to limit physical access to ePHI and the facilities in which they are housed *[Section 164.310(a)(1)]*	▪ **Contingency Operations** – procedures allowing facility access in the event of emergency under disaster plan and emergency mode operations plan	(A)	11	✓			✓
	▪ **Facility Security Plan** – policies and procedures to safeguard the facility and equipment from unauthorized access, tampering, and theft	(A)	11	✓			✓
	▪ **Access Control and Validation Procedures** – procedures to control and validate access to facilities based on role or function, including visitor control and control of access to software programs for testing and revision	(A)	11	✓			✓
	▪ **Maintenance Records** – policies and procedures to document repairs and modifications performed on facility components related to physical security	(A)	11	✓			✓
Workstation Use: Policies and procedures specifying the functions staff are permitted to perform on their workstations, the manner in which the functions are performed, and the physical attributes of the surroundings of workstations with access to ePHI *[Section 164.310(b)]*		(R)	12, 20	✓			✓
Workstation Security: Policies and procedures to limit access to workstations to authorized users *[Section 164.310(c)]*		(R)	13	✓			✓

STANDARDS	IMPLEMENTATION SPECIFICATIONS	(R) =REQUIRED (A) =ADDRESSABLE	POL #	ALREADY IN PLACE	CUSTOMIZE P&P	NOT IMPLEMENTING	TRAINING COMPLETE
Device and Media Controls: Policies and procedures related to moving hardware and electronic media in and out of the facility, and within the facility *[Section 164.310(d)(1)]*	▪ **Disposal** – policies and procedures dealing with the safeguarding of ePHI being disposed of, including the disposal of hardware and other media ▪ **Media Re-use** – policies and procedures addressing the removal of ePHI being reused ▪ **Accountability** – maintaining a record of the movements of hardware and electronic media and documentation of persons responsible ▪ **Data Back-up and Storage** – create a retrievable copy of ePHI, if needed, before movement of equipment	(R)	14	✓			✓
		(R)	14	✓			✓
		(A)	14	✓			✓
		(A)	14	✓			✓

Technical Safeguards

Standards	Implementation Specifications	(R) =Required (A) =Addressable	Pol #	Already in Place	Customize P&P	Not Implementing	Training Complete
Access Control: Implement technical policies and procedures ensuring access to ePHI to individuals who have been granted access *[Section 164.312(a)(1)]*	▪ **Unique User Identifier** – assign unique name and/or number for identifying and tracking user identity ▪ **Emergency Access Procedure** – policies and procedures identifying ways to access ePHI during emergencies ▪ **Automatic Logoff** – electronic procedures that automatically disconnect electronic sessions after predetermined periods of inactivity ▪ **Encryption and decryption** – implementation of mechanisms to encrypt and decrypt ePHI to prevent unauthorized use	(R)	15	✓			✓
		(R)	15	✓			✓
		(A)	15	✓			✓
		(A)	15	✓			✓
Audit Controls: Implement mechanisms that record and examine activity in information systems that contain or use ePHI *[Section 164.312(b)]*		(R)	16	✓			✓
Integrity: Policies and procedures to protect against the improper alteration or destruction of ePHI *[Section 164.312(c)(1)]*	▪ **Mechanism to authenticate electronic protected health information** – implement electronic mechanisms to corroborate that the ePHI has not been altered or destroyed	(A)	17	✓			✓
Person or Entity Authenti-cation: Procedures to verify that persons or entities seeking access to ePHI are the ones claimed *[Section 164.312(d)]*		(R)	18	✓			✓

STANDARDS	IMPLEMENTATION SPECIFICATIONS	(R) =REQUIRED (A)=ADDRESSABLE	POL #	ALREADY IN PLACE	CUSTOMIZE P&P	NOT IMPLEMENTING	TRAINING COMPLETE
Transmission Security: Implement measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network *(Section 164.312(e)(1)*	▪ **Integrity Controls** – ensure that electronically transmitted ePHI is not modified without detection	(A)	19	✓			✓
	▪ **Encryption** – implement mechanisms to encrypt ePHI whenever appropriate	(A)	19	✓			✓

Susan Lee 7/11/16