HIPAA Compliance Checklist

HIPAA Security Rule	Standard Description (R) Required Standard (A) Addressable Standard	Yes / No / NA
Administrative Safeguards		
§ 164.308(a)(1)(i) Security Management Process	(R) Have you implemented policies and procedures to prevent, detect, contain, and correct security violations?	
§ 164.308(a)(1)(ii)(A) Risk Analysis	(R) Have you conducted a Risk Analysis that includes Administrative, Physical, and Technical Safeguards?	
§ 164.308(a)(1)(ii)(B) Risk Management	(R) Do you have a Risk Management plan that contains the dates when you mitigated the vulnerabilities?	
§ 164.308(a)(1)(ii)(C) Sanction Policy	(R) Do you have a tiered sanction policy for employees who have violated your HIPAA privacy and security policies and procedures?	
§ 164.308(a)(1)(ii)(D) Information System Activity Review	(R) Do you have documented procedures for reviewing user activity within information systems that contain or access ePHI?	
§ 164.308(a)(2) Assigned Security Responsibility	(R) Have you assigned a Security Officer to implement and enforce Security Policies and Procedures?	

§ 164.308(a)(3)(i) Workforce Security	(R) Do you have written policies and procedures in place to determine the level of access to ePHI for each employee?	
§ 164.308(a)(3)(ii)(A) Authorization and/or Supervision	(A) Do you have procedures in place for the authorization and/or supervision of employees who work with ePHI or in locations where it might be accessed?	
§ 164.308(a)(3)(ii)(B) Workforce Clearance Procedure	(A) Do you have documented procedures to determine appropriate access to ePHI for employees?	
§ 164.308(a)(3)(ii)(C) Termination Procedures	(A) Do you have documented procedures to terminate access to ePHI when a user is no longer authorized to access?	
§ 164.308(a)(4)(i) Information Access Management	(R) Have you implemented policies and procedures for authorizing access to ePHI?	
§ 164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Functions	(R) If your organization is a Clearinghouse and is part of a larger organization, have you implemented policies and procedures to protect ePHI from the larger organization?	
§ 164.308(a)(4)(ii)(B) Access Authorization	(A) Have you implemented policies and procedures for granting access to ePHI through particular workstations, programs, or other processes?	

§ 164.308(a)(4)(ii)(C) Access Establishment and Modification	(A) Based on your access authorization policies and procedures, do you have a process in place to modify a user's access to ePHI whether it is through a workstation, software program, or particular process?	
§ 164.308(a)(5)(i) Security Awareness and Training	(R) Do you have a documented security awareness and training program in place for your staff including management?	
§ 164.308(a)(5)(ii)(A) Security Reminders	(A) Do you have documented Security Reminders?	
§ 164.308(a)(5)(ii)(B) Protection from Malicious Software	(A) Do you have documented policies and procedures for the detection, protection, and reporting of malicious codes?	
§ 164.308(a)(5)(ii)(C) Log-in Monitoring	(A) Do you have procedures in place for monitoring and reporting login attempts?	
§ 164.308(a)(5)(ii)(D) Password Management	(A) Do you have documented procedures for creating, changing, and safeguarding passwords? If so, do you require strong passwords or passphrases to be utilized?	
§ 164.308(a)(6)(i) Security Incident Procedures	(R) Have you implemented policies and procedures to address security incidents?	

§ 164.308(a)(6)(ii) Response and Reporting	(R) Do you have a process in place to identify, mitigate, and report suspected or known security incidents?	
§ 164.308(a)(7)(i) Contingency Plan	(R) Have you established and implemented policies and procedures for responding to an emergency or disaster that could damage or destroy ePHI?	
§ 164.308(a)(7)(ii)(A) Data Backup Plan	(R) Do you have a documented data backup plan to create and maintain exact copies of all portions of ePHI?	
§ 164.308(a)(7)(ii)(B) Disaster Recovery Plan	(R) Have you established and implemented procedures to restore any loss of data?	
§ 164.308(a)(7)(ii)(C) Emergency Mode Operation Plan	(R) Have you established and implemented procedures to enable the continuation of critical business processes for the protection of ePHI while operating in an emergency mode?	
§ 164.308(a)(7)(ii)(D) Testing and Revision	(A) Have you implemented procedures to test, evaluate, and revise your contingency plan?	
§ 164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis	(A) Have you created a list of specific applications and data and assessed the criticality of each component?	

§ 164.308(a)(8) Evaluation	(R) Do you have a schedule to review your technical and nontechnical standards that affect the security of your ePHI and your facility that it is housed in?	
§ 164.308(b)(1) Business Associate Contracts	(R) Do you have business associate agreement in place with all entities that create, receive, maintain, or transmit ePHI?	
§ 164.308(b)(4) Written Contract or Other Arrangement	(R) Do you have written service contracts with those entities that outline the security requirements of ePHI or do you have documented assurances that demonstrate they are compliant with the HIPAA rules?	
Physical Safeguards		
§ 164.310(a)(1) Facility Access Control	(R) Do you have policies and procedures that limit physical access to ePHI and the facility that ePHI is housed in?	
§ 164.310(a)(2)(i) Contingency Operations	(A) Have you established and implemented procedures that allow access to the facility during the restoration process under the disaster recovery and emergency mode operations plan?	
§ 164.310(a)(2)(ii) Facility Security Plan	(A) Have you implemented policies and procedures to safeguard the facility and equipment from unauthorized access, tampering, and theft?	

§ 164.310(a)(2)(iii) Access Control and Validation Procedures	(A) Have you implemented procedures to control and validate a person’s access to facilities and software programs and is this based on their function or role? This includes employees and visitor access.	
§ 164.310(a)(2)(iv) Maintenance Records	(A) Do you have policies and procedures to document repairs and/or physical modifications to the facility which are related to security?	
§ 164.310(b) Workstation Use	(R) Do you have policies and procedures that specify proper functions that are permitted with the use of workstations that access ePHI?	
§ 164.310(c) Workstation Security	(R) Have you implemented physical safeguards for all workstations and devices to restrict access to ePHI to only authorized users?	
§ 164.310(d)(1) Device and Media Controls	(R) Do you have policies and procedures that document the movement and transportation of hardware and electronic media in and out of the facility and movement within the facility that contain ePHI?	
§ 164.310(d)(2)(i) Disposal	(R) Do you have policies and procedures for the disposal of hardware or electronic media that contains or has contained ePHI?	

§ 164.310(d)(2)(ii) Media Re-use	(R) Do you have policies and procedures for the removal of ePHI from hardware or electronic media before it is available for re-use?	
§ 164.310(d)(2)(iii) Accountability	(A) Do you maintain a record of movement of hardware and electronic media and the person that is responsible?	
§ 164.310(d)(2)(iv) Data Backup and Storage	(A) Do you have procedures in place to create an exact copy of ePHI before the movement of equipment?	
Technical Safeguards		
§ 164.312(a)(1) Access Control	(R) Have you implemented technical policies and procedures for information systems that maintain ePHI and only allow access to those persons or software programs that have been granted access rights?	
§ 164.312(a)(2)(i) Unique User Identification	(R) Have you assigned a unique name or number for all users to enable identification and tracking purposes?	
§ 164.312(a)(2)(ii) Emergency Access Procedure	(R) Have you established and implemented procedures for obtaining access to ePHI during an emergency?	

§ 164.312(a)(2)(iii) Automatic Logoff	(A) Have you implemented electronic procedures to terminate an electronic session after a predetermined time of inactivity?	
§ 164.312(a)(2)(iv) Encryption and Decryption	(A) Have you implemented a process that encrypts and decrypts ePHI when it is transmitted?	
§ 164.312(b) Audit Controls	(R) Do you utilize hardware, software, or have procedure in place that can record and examine activity in systems that use or have access to ePHI?	
§ 164.312(c)(1) Integrity	(R) Have you implemented policies and procedures to protect ePHI from improper alteration or destruction? These include technical and non-technical sources.	
§ 164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information	(A) Do you utilize electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?	
§ 164.312(d) Person or Entity Authentication	(R) What type of authentication do you utilize to ensure the validity of an individual’s claim that he/she has been authorized access to ePHI?	

§ 164.312(e)(1) Transmission Security	(R) Have you implemented technical measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network?	
§ 164.312(e)(2)(i) Integrity Controls	(A) Have you implemented security measures to ensure that ePHI is not improperly modified without detection until disposed of?	
§ 164.312(e)(2)(ii) Encryption	(A) Have you implemented a mechanism to encrypt ePHI whenever deemed appropriate such as in transit and at rest on all devices?	
Organizational Requirements		
§ 164.314(a)(1) Business Associates Contract or Other Arrangements	(R) Do your BA agreements have specific criteria that are required?	
§ 164.314(a)(2)(i) Business Associate Contracts	(R) Do your BA agreements state how the BA will implement administrative, physical, and technical safeguards and include any subcontractors will follow the same guidelines?	
§ 164.314(a)(2)(ii) Other Arrangements	(R) Are you a governmental agency? If so, are any of your Business Associates?	
§ 164.314(b)(1) Requirements for Group Health Plans	(R) Are you a group health plan or part of a self-insured health plan?	

§ 164.314(b)(2) Implementation Specifications	(R) If so, have you implemented administrative, physical, and technical safeguards? Do your safeguards adequately separate information according to § 164.504(f)(2)(iii)? Do you have contracts in place to ensure any agent that provides the information agrees to appropriately implement security measure to protect the information? Do you have procedures to report a security incident to the plan?	
Policies and Procedures and Documentation Requirements		
§ 164.316(a) Policies and Procedures	(R) Do you have reasonable and appropriate policies and procedures that comply with the Security Standards?	
§ 164.316(b)(1) Documentation	(R) Do you maintain appropriate documentation that demonstrates your compliance efforts?	
§ 164.316(b)(2)(i) Time Limit	(R) Do you retain the documentation for at least 6 years from the date of its creation or the last it was last in effect?	
§ 164.316(b)(2)(ii) Availability	(R) Have you made your policies, procedures, and documentation available for those who need access?	
§ 164.316(b)(2)(iii) Updates	(R) Do you review your policies, procedures, and documentation periodically and update as needed in response to	

	operational or environmental changes?	
Mobile Device Management and Remote Access		
§ 164.306(b)(2)	(R) Have you evaluated your need to off-site use or access to ePHI and have you considered security factors that will be required?	

Recognized Security Standards		
Public Law 116-321 Security standards, guidelines, best practices, methodologies, and procedures developed under the National Institute of Standards and Technology (NIST)	(R) Do you have documentation of your data security compliance efforts for a minimum of one year?	

HIPAA Privacy Rule		
§ 164.528 Accounting of Disclosures	(R) Do you have procedures and forms when a patient requests an accounting of disclosures?	
§ 164.522(b) Confidential communication by alternate means	(R) Do you have included in your intake forms a section that asks where and how a patient prefers to be contacted?	
§ 164.506 Designated Record Set	(R) Have you implemented policies and procedures that explain what is included in the designated record set and how a patient may request their records?	

§ 164.502(b), § 164.514 Minimum necessary standard	(R) Do you have policies that explain what the minimum necessary standard means and how it must be applied?	
§ 164.520 Notice of privacy practices for office and website	(R) Do you have an updated version of your notice of privacy practices in the office and on your website?	
§ 164.524 Patient right of access to protected health information (PHI)	(R) Do you have documented procedures that includes a timely response time when a patient requests access to their medical information?	
§ 164.526 Patient request to amend their protected health information (PHI)	(R) Do you documented procedures and forms when a patient requests their medical information to be amended?	
§ 164.522 Patient request to restrict access to protected health information (PHI)	(R) Do you have procedures and forms when a patient requests a restriction for services they have paid for in full out of pocket?	

Information Blocking Rule		
ONC's Cures Act (21st Century Cures Act) Interoperability Requirements	(R) Do your information technology partners ensure a patient can receive their medical records in the app (format) of their choice?	
	(R) Have you implemented procedures that explain how to a patient may request their medical records in the app of their choice?	