Sample HIPAA Security Risk Assessment For a Small Physician Practice

Administrative, Physical, and Technical Safeguards
Breach Notification Rule

How to Use this Risk Assessment

The following sample risk assessment provides you with a series of sample questions to help you prioritize the development and implementation of your HIPAA Security policies and procedures. While this risk assessment is fairly lengthy, remember that the risk assessment is required and it is critical to your compliance with the Security Rule. These sample questions cover Administrative, Physical, and Technical Safeguards, and the Breach Notification Rule, and are only representative of the issues you should address when assessing different aspects of your practice. Keep your completed risk assessment documents in your HIPAA Security files and retain them in compliance with HIPAA document retention requirements.

HIPAA Security requires Covered Entities to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic Protected Health Information ("ePHI") and to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. ***Assessing risks is only a first step. You must use the results of your risk assessment to develop and implement appropriate policies and procedures.***

This form is educational only, does not constitute legal advice, and covers only federal, not state, law.

Sample Risk Analysis Directions:

1. Review each of the following sample questions and rank the level of risk on a scale of 1 to 6 (with 1 being the lowest level of risk and 6 being the highest level of risk)

    a. "Risk for us" — 5 or 6 on your rating scale. You believe the situation or activity could put your practice at risk. For example, if your portable computer or smart phone contains scheduling or patient information, you have a high risk of exposing patient information if the ePHI it contains is not encrypted.

    b. "Could be a risk" — 3 or 4 on your rating scale. For example, a poorly maintained inventory of electronic equipment would put you at risk of not being able to reconstruct your practice for an insurance claim in the event of a disaster.

    c. "Not a risk" — 1 or 2 on your rating scale. For example, the risk of flooding is likely to be lower for a physician practice that is located in a low flood risk area than for a practice located in a high flood risk area.

2. The following sample questions are designed to illustrate the kinds of questions that a physician practice should analyze in conducting its HIPAA Security Risk Analysis. Similar sample questions may appear in several sections because the sample questions correspond with various provisions of the Security Rule and are intended to allow you to think through your risks in different ways.

3. Identify a Security Official to develop and implement security policies and procedures and to oversee and protect confidential health information. For example, mobile computers often score a 5-6 risk rating. The Security Official should confirm that ePHI stored on such hardware is encrypted, and all such hardware is accounted for through either a check-in/check-out process or by storage in a locked cabinet at the end of each day.

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	

Administrative Safeguards

Security Management Process 164.308(a)(1) Team: Security Official, Physician, Workforce Members								
Risk Analysis	Required							
		Do you keep an updated inventory of hardware and software owned by the practice?						
		Can you identify where ePHI is located (e.g., desktops, laptops, handhelds, tablets, removable media, servers, etc.)?						
		Could you locate the inventory in a disaster (fire, flood, explosion, theft)?						
		Do you know the current approximate value of your hardware and software?						
		Does the inventory contain all necessary contact information, including information for workforce members and service providers?						
		Do you control the information contained on your information system?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you or your workforce take home portable computers or other devices containing ePHI?						
		Does any vendor have access to confidential patient data? Have you discussed HIPAA Security and HITECH requirements with such vendor(s)? Is an up-to-date Business Associate Agreement in place for each vendor that has access to ePHI?						
		Can a vendor change confidential patient data? If so, are you monitoring audit logs for such changes?						
Risk Management	Required							
		Do you update your workforce members' training each time you develop and implement new policies and procedures? Do you document initial and continuing training?						
		Have you set user access to ePHI? Does access correspond to job descriptions (clinical, administrative, billing)?						
		Do you monitor reports that identify persons and systems that access ePHI,						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		including those not authorized to have access to ePHI?						
		Do you have control over who can amend your patient records?						
Sanctions Policy	Required							
		Have you developed a written sanctions policy against workforce members who do not abide by your policies?						
		Have you explained those sanctions to your workforce members?						
		Do you consistently enforce those sanctions?						
Information System Activity Review	Required							
		Do you regularly review system audit trails that identify who has accessed the system and track additions, deletions, or changes they may have made to ePHI?						
		Would you know if someone was trying to hack into your system? (Do you regularly review security incident reports?)						
Assigned Security Responsibility 164.308(a)(2)								

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
Team: Physician, Security Official, Privacy Official								
Assigned Security Responsibility	Required							
		Have you appointed a Security Official?						
		Do your Privacy and Security Officials coordinate privacy and security policies and procedures? (Privacy and Security Official may be the same person)						
Workforce Security 164.308(a)(3) Team: Security Official, Privacy Official								
Authorization and/or Supervision	Address-able							
		Do you have written job descriptions that define appropriate access to ePHI?						
		Could an unauthorized workforce member obtain access to ePHI?						
		Are persons with access to ePHI supervised?						
Workforce Clearance Procedure	Address-able							
		Do you contact references before hiring employees?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you conduct background checks?						
Termination Procedures	Address-able							
		Do you immediately deactivate a workforce member's access upon termination (or, as appropriate, upon change of job description)?						
		Do you notify your IS vendor of an employee's termination within a specific time?						
		Is there a standard checklist of action items when an employee leaves? (Return keys, close and payment of credit cards, return software and hardware)						
		Does your practice consistently enforce checklists and policies with respect to all employees who are terminated or whose duties have changed, whether the termination or change was voluntary or for cause?						
Information Access Management 164.308(a)(4) Team: Security Official, Physician								
Isolating Health Care Clearinghouse	Required							

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
Functions								
		If you use a health care clearinghouse that is part of a larger organization, have you confirmed that the clearinghouse has implemented policies and procedures to protect ePHI from unauthorized access by the larger organization?						
Access Authorization	Address-able							
		Are you using your IT system's log-in process to authorize access (such as limiting administrative access)?						
		Is each workforce member's access to ePHI based on his or her job description?						
Access Establishment and Modification	Address-able							
		Do you document, periodically review, and modify as appropriate workforce members' access to ePHI?						
Security Awareness and Training 164.308(a)(5) Team: Security Official, with input from Privacy Official								
		Have you implemented a security awareness and training program for all members of your workforce, including						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		management?						
Security Reminders	Address-able							
		Have there been lapses in privacy safeguards that indicate a need for training refreshers?						
		Have you identified your security training priorities?						
		Are security reminders posted in a visible location?						
		Are vendors aware of your security reminders?						
		Do workforce members know where to find a copy of your security policies and procedures?						
		Do workforce members understand the consequences of noncompliance with those policies?						
		Are workforce members with laptops, PDAs, or cell phones aware of encryption requirements?						
		Do you consistently follow your security awareness and training program with all new hires?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
Protection from Malicious Software	Address-able							
		Have you installed anti-virus and other anti-malware protection software on your computers? Do you use it to guard against, detect, and report any malicious software? Do you protect against spyware?						
		Do workforce members update the virus protection software when it is routed to them?						
		Do you prohibit workforce members from downloading software they brought in from elsewhere? (digital family photos, games, books, music, etc.)						
Log-in Monitoring	Address-able							
		Does the Security Official regularly monitor audit logs?						
		Is the Security Official notified of unsuccessful log-ins?						
		Do workforce members know what to do if they cannot access the system?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
Password Management	Address-able							
		Have you established procedures for creating, changing, and safeguarding passwords?						
		Are sanctions in place if workforce members share passwords?						
		Do workforce members know what to do if they forget a password?						
		Are you providing password management reminders?						
Security Incident Procedures 164.308(a)(6) Team: Security Official, Practice Management Vendor								
Response and Reporting	Required							
		Do you know if your security system has ever been breached?						
		Have you prioritized what must be restored in the event of a system disruption?						
		Have you developed a list of persons and entities to contact in the event of a security incident?						
		Do you require workforce members to tell you immediately if they suspect a						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		compromise to your system?						
		Have you made a list of possible security incidents?						
		Do you document all security incidents and their outcomes?						
Contingency Plan 164.308(a)(7) Team: Security Official, Privacy Official, Physician								
Data Backup Plan	Required							
		Does your practice back up its electronic data?						
		Do you store the backup data at the physician practice's location?						
		Do you know whom to call to restore data?						
Disaster Recovery Plan	Required							
		Do you have a procedure to restore any loss of data?						
		Do you have a list of critical hardware, software, and workforce members?						
Emergency Mode Operation Plan	Required							
		If you are required to operate in emergency mode, do you have procedures to enable you to continue						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		critical business processes to protect the security of ePHI?						
		Do you have a plan to temporarily relocate if you lose access to your physical location?						
		Would ePHI be safeguarded in this temporary location?						
		Are formal agreements in place for such a relocation?						
		Have you trained staff on your contingency plan?						
		Is there a contingency plan coordinator?						
		Do you have an emergency call list?						
		Have you identified situations in which your contingency plan must be activated?						
		Is there a plan to restore systems to your normal operations?						
Testing and Revision Procedures	Address-able							
		Have you tested your contingency plan?						
Applications and Data Criticality Analysis	Address-able							

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you have a plan to restore your business activities, beginning with what is most critical to your practice?						
Evaluation 164.308(a)(8) Team: Security Official, Privacy Official, Physician								
Evaluation	Required							
		Do you perform periodic HIPAA Security evaluations?						
		Do you perform these evaluations in response to environmental and operations changes affecting the security of your ePHI, to determine whether your security policies and procedures meet HIPAA Security requirements?						
		Do you perform both technical and nontechnical evaluations?						
		Has your Security Official determined acceptable levels of risk in its business operations and mitigation strategies?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you have a plan to evaluate your systems at least annually, or at any time a risk warrants a review?						
Business Associate Contracts and Other Arrangements 164.308(b)(1) Team: Security Official, Privacy Official, Physician								
Written Business Associate Contract	Required							
		Are all necessary Business Associate Agreements in place? Are they HIPAA and HITECH compliant?						
		Are there new organizations or IT vendors that require a Business Associate Agreement?						
Physical Safeguards								
Facility Access Controls 164.310(a)(1) Team: Security Official, Privacy Official, Physician								
Contingency Operations	Address-able							
		Do you know who needs access to the facility in the event of a disaster?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you have a backup plan for access, including who has authority to access the facility in a disaster?						
Facility Security Plan	Address-able							
		Do you have an inventory of facilities and equipment therein?						
		How do you safeguard your facility and equipment from unauthorized physical access, tampering, and theft?						
		Is there a contingency plan in place?						
Access Control and Validation Procedures	Address-able							
		Do you have procedures in place to control physical access to your facility and areas within your facility where ePHI could be accessed?						
		Do you validate a person's authority to access software programs for testing and revision?						
		Is there a history or risk of break-ins that requires monitoring equipment?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		If monitoring or surveillance equipment generates records or footage, how is it reviewed, handled, and disposed of?						
		If you use a security contractor for surveillance purposes, do you have an up-to-date Business Associate Agreement in place with the contractor?						
Maintenance Records	Address-able							
		Have you repaired or modified any physical components of your facility related to security, such as doors, locks, walls, or hardware, or do you expect to do so?						
		Do you have a system to document all such repairs and modifications?						
Workstation Use 164.310(b) Team: Security Official, Privacy Official, Physician								
Workstation Use	Required							
		Have you documented how workstations are to be used in the physician practice?						
		Are there wireless tools used as workstations?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Can unauthorized persons view content of workstations?						
Workstation Security 164.310(c) Team: Security Official, Privacy Official, Physician, IT Vendor								
Workstation Security	Required							
		Is access to ePHI restricted to authorized users?						
		Is there a log-off policy before leaving computers unattended?						
		Is there a policy that controls Internet access while working with ePHI?						
Device and Media Controls 164.310(d)(1) Team: Security Official, Privacy Official, Physician, IT Vendor								
Disposal	Required							
		Do you destroy data on hard drives and file servers before disposing the hardware?						
Media Re-use	Required							
		Are workforce members trained as to the security risks of re-using hardware and software that contain ePHI?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you have a procedure for removing ePHI from electronic media before it can be re-used?						
Accountability	Address-able							
		Do you document the movement of hardware and electronic media and who is responsible for each item?						
		Do you periodically check the inventory to ensure computers are where they are supposed to be?						
		Do you document where they've been moved?						
		Is the inventory list part of your disaster recovery files? Is it stored in a disaster-proof manner, i.e., offsite and (preferably) electronically?						
Data Backup and Storage	Address-able							
		Do you regularly back up data on hardware and software and maintain backup files off site?						
		Do you back up ePHI before equipment is moved?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Have staff members been trained on backup policies?						
Technical Safeguards								
Access Control 164.312(a)(1) Team: Security Official, Privacy Official, Physician, IT Vendor								
Unique User Identification	Required							
		Has the Security Official assigned a unique user identity to each member of the workforce?						
		Are passwords unique to each individual and not shared?						
		Is there a sanction policy on sharing passwords?						
		Do workforce members have access to the minimum ePHI necessary to perform their job responsibilities?						
		Do you participate in ePrescribing? If so, does the system validate your electronic signature? Are physicians the only providers allowed to ePrescribe in your practice?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
Emergency Access Procedure	Required							
		Does the Security Official have a unique user ID that is used only in emergencies?						
		Is there a process to notify another leader in the practice when the emergency ID is used?						
Automatic Logoff	Address-able							
		Do your computers automatically log off after a specific period of inactivity?						
		Is there a shorter log off period for computers in high traffic areas?						
Encryption and Decryption	Address-able							
		Do you send e-mail containing ePHI to patients?						
		Is the e-mail sent over an open network such as AOL, Yahoo!, EarthLink, or Comcast?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Do you have a mechanism in place to encrypt and decrypt ePHI?						
Audit Controls 164.312(b) Team: Security Official, IT Vendor								
Audit Controls	Required							
		Is there a procedure in place to monitor and audit workforce members with access to ePHI and their activity with respect to ePHI?						
		Is one person responsible for conducting audit processes and reporting results?						
		Has your IT vendor explained how to conduct audits?						
Integrity 164.312(c)(1) Team: Security Official, Privacy Official, Physician, IT Vendor								
Mechanism to Authenticate ePHI	Address-able							
		Are users required to authenticate themselves when logging on to the system?						
		Is there a feature that locks out users after a specific number of failed log-in attempts?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Is data transmitted through standard network protocols?						
		Have you identified sources that would jeopardize the integrity of ePHI (vandalism, hackers, system failures, viruses)?						
		Is there an electronic mechanism to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?						
Person or Entity Authentication 164.312(d) Team: Security Official, Privacy Official, Physician, IT Vendor								
Person or Entity Authentication	Required							
		Does your system require users to identify themselves using a password and user name?						
		Does the system allow you to conduct audit trails on users?						
Transmission Security 164.312(e)(1) Team: Security Official, IT Vendor								
Integrity Controls	Address-able							
		Does the software allow you to track and audit users who transmit and alter ePHI?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Is there an auditing process in place?						
		Does the IT vendor ensure that information is not altered in transmission?						
Encryption	Address-able							
		Does your practice use a mechanism (secure network) to encrypt e-mail or other ePHI?						
		Does your practice send ePHI via handhelds or wireless laptops?						
		Do workforce members know how to respond to e-mails containing ePHI?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	

Breach Notification Rule

Notification in the Case of Breach of Unsecured Protected Health Information ("PHI") 45 CFR Part 164 Subpart D Team: Security Official, Physician, Workforce Members								
		Are paper charts or portable computers containing PHI ever taken out of the practice? This includes portable computers, back-up tapes, smart phones, paper charts.						
		Are electronic devices encrypted? Do you periodically check electronic equipment to ensure encryption safeguards have not been disabled?						
		How does your practice "secure" non-electronic PHI ("secure" has a specific meaning under the Breach Notification Rule) and protect oral PHI?						
		Is your workforce trained to immediately report suspected breaches of PHI?						

Sample HIPAA Security Risk Assessment
For a Small Physician Practice

Implementation Specification	R/A	Sample Risk Assessment Question	Risk			Policy		Assigned to
			Risk for us	Could be a risk	Not a risk	Policy in place	Need policy	
		Does your practice have a procedure in place to conduct a risk analysis of any suspected breaches of PHI?						
		Have you asked your Business Associates what they are doing to comply with the Breach Notification Rule?						
		Have you updated your Business Associate Agreements to require your Business Associates to notify you promptly if they discover a breach of PHI and to provide you with all of the appropriate information regarding the breach?						