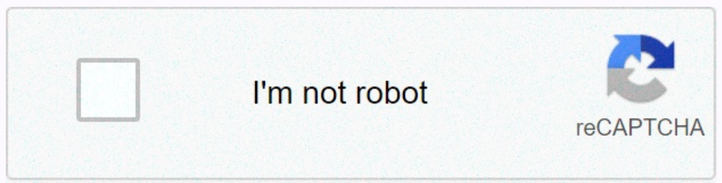


Continue

# Security risk assessment template for meaningful use

Safety Risk Assessment Tool, hipa/HITECH assessment toolkit Safety risk analysis is a systematic and ongoing process of identifying and examining potential threats and vulnerabilities to protected health information and making changes to make patient health data more secure. Hipaa's privacy and safety rule requires health organizations to actively prevent risks and protect patient privacy to ensure patient privacy.2.1 Risk Assessment Questionnaire: This online risk assessment questionnaire, which consists of several technology areas, is designed to support the requirements of the Department of Health and Human Services (HHS), the Office of Civil Liberties (OCR), the NIST and other relevant data protection laws and regulations. 2.2 Risk management: The risk management action plan aims to organise and prioritise identified risks on the basis of probability and impact criteria. Firstly, the risks that are of paramount importance must be mitigated. 2.3 Templates for policies and procedures: For the implementation of security controls, a list of updated templates from NIST, CIS, and other authoritative organizations is used. All relevant organizations and business partners must comply with HIPAA/HITECH's privacy, security and privacy rules, which specifically focus on protecting the confidentiality, integrity and availability of electronic protected health information (ePHI). As part of this requirement, EHR 2.0 has developed an easy-to-use HIPAA/HITECH online toolkit for small organizations to evaluate privacy, security, and breach requirements. Our toolkit consists of: 3.1 ePHI Inventory Template: The first step in hipaa/hitech evaluation is to identify ePHI systems, processes and persons involved in the creation, reception, maintenance and transmission of ePHI. This template helps organizations develop the ePHI master set. 3.2 Sample Information Policies and Procedures: HIPPA Safety Guidelines reflect the rules on electronic protected health information (ePHI) treatment procedures. This includes, but is not limited to, physical security policy, technology security policy, sanctions policy, access policy, emergency plans, security incident procedures and social media section. 3.3 HIPAA/HITECH evaluation checklist: This easy-to-use HIPAA/HITECH safety rules checklist includes all 28 administrative safeguards, 12 physical safeguards and 12 technical safeguards. This evaluation checklist helps health organizations with the necessary and addressable HIPAA/HITECH security rules, in addition to privacy and breach rules. 3.4 Chart 2: This flowchart is designed to take a consistent approach to risk assessment and to determine whether infringement notifications are being Health information (PHI).3.5 HIPAA training for staff: This online training module covers all important areas of HIPAA awareness training for health personnel with evaluation questions and a performance certificate. Risk Assessment QuestionnaireRisk Management Plan Policies and Procedurs TemplateStaff Awareness TrainingSy reasonable use, MIPS and MACRA Security Risk Assessment Measure Includes the Security Risk Assessment Tool, aHIPAA/HITECH Privacy RuleHIPAA/HITECH Security RuleHIPAA/HITECH Breach RuleCompliance Portal The NIST HIPAA Security Toolkit application, developed by the National Institute of Standards and Technology (NIST), aims to help organizations better understand hipaa security rule requirements, implement these requirements, and evaluate implementations in their operating environments. Target users include, but are not limited to, hipaa entities, business partners, and other organizations, such as organizations that implement, evaluate, and provide compliance services to the HIPAA security rule. The Office of the National Coordinator for Health Information Technology (ONC) and the Civil Rights Office (OCR) of HHS have jointly launched a HIPAA Safety Risk Assessment Tool. The tool's features make it useful to help small and medium-sized health practices and business partners comply with the Health Insurance Portability and Accountability Act (HIPAA) safety rule. The Office of Civil Rights (OCR) is responsible for issuing periodic guidelines for the provisions of the HIPAA security rule. (45 C.F.R. §§ 164.302 to 318) This set of guidance documents will help organisations identify and implement the most effective and appropriate administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic protected health information. The materials shall be updated annually as necessary. For more information, see our other safety rule guidance material and faq for the safety rule. Download a copy of this guide in PDF. Introduction The Civil Rights Office (OCR) is responsible for issuing annual guidance on the provisions of the HIPAA security rule.1 (45 C.F.R. §§ 164.302 – 318. This set of guidelines will help organisations2 to identify and implement the most effective and appropriate administrative, physical and technical safeguards necessary to provide electronic protected health information (e-PHI). Guidance materials shall be developed with the consent of stakeholders and the public and updated as necessary. The series shall begin with the risk analysis required in paragraph 164.308(a) 1(ii) (A). Carrying out risk analysis is the first step in the safety rule to comply with standards and implementation identification and implementation of appropriate safeguards. Therefore, risk analysis is essential and needs to be understood in detail before provide meaningful guidance that specifically manages safeguards and technologies that best protect electronic health information. The guide is not intended to provide a uniform plan for compliance with the risk analysis requirement. Instead, it clarifies the Department's expectations for organizations working to meet these requirements.3 The organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and the environment. We note that some of the content in this guide is based on the recommendations of the National Institute of Standards and Technology (NIST). The nist federal agency publishes freely available material to the public, including policies.4 While only federal agencies must follow NIST's guidelines, the guidelines represent an industry standard for good business practices for standards for ensuring e-PHI. Therefore, non-federal organizations may find their content valuable in the development and implementation of compliance activities. All e-PHI created, received, maintained, or forwarded by the organization are subject to the security rule. The security rule requires entities to assess the risks and vulnerabilities in their environment and to implement reasonable and appropriate security measures against reasonably expected threats or threats to the security or integrity of e-PHI. Risk analysis is the first step in the process. We understand that the security rule does not provide for a specific risk analysis method, recognising that methods can vary depending on the size, complexity, and capabilities of your organization. Instead, the rule defines risk analysis as a fundamental element in achieving compliance and sets out a number of objectives that any accepted methodology must achieve. Security rule risk analysis requirements The security rule security management process standard requires organizations to establish [i]mplement policies and procedures to prevent, detect, reduce, and improve security breaches. (45 C.F.R. § 164.308 (a) (1)) Risk analysis is one of four necessary implementation requirements that provide instructions for implementing the safety management process standard. Section 164.308( a) (1) (ii) (A) states: RISK ANALYSIS (Mandatory). Accurately and thoroughly assess the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information held by [the organisation]. The following questions, brought forward by the NIST 800-665 specialist published (SP), are examples that organizations may consider risk analysis. These sample questions are not prescriptive and only address problems that are which an organization wants to take into account when implementing the security rule: • Have you identified e-PHI within the organization? This includes the e-PHI, e-PHI, maintenance or transmission. • What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain, or transmit e-PHI? • What are the human, natural and environmental threats to information systems containing e-PHI? In addition to the explicit requirement for risk analysis, the rule also indicates that risk analysis is a necessary tool to achieve significant compliance with a number of other standards and implementing requirements. For example, the rule contains several implementation specifications that are labeled addressable instead of mandatory. (68 FR 8334, 8336 (20 February 2003).) The addressable implementing requirement shall not be optional; rather, if an organisation finds that the implementation requirement is not reasonable and appropriate, the organisation should document why it is not reasonable and appropriate and adopt equivalent action if this is reasonable and appropriate. (See 68 FR 8334, 8336 (February 20, 2003); 45 C.F.R. § 164.306(d)[3]) The outcome of the risk analysis process is a critical factor in assessing whether an implementing requirement or equivalent measure is reasonable and appropriate. For example, organisations should use the information collected from their risk analysis as follows: • Design appropriate staff screening procedures. (45 C.F.R. § 164.308(a) 3) (ii) the commission shall be (B)) • Determine what data to back up and how. (45 C.F.R. § 164.308 (a) 7.(ii)(A)) • Decide whether and how to use encryption. (45 C.F.R. §§ 164.312(a) 2. • In order to protect the integrity of the data, it is necessary to specify what data should be authenticated in certain situations. (45 C.F.R. § 164.312(c) (2)) • Determine the appropriate way of transmitting health information. (45 C.F.R. § 164.312(e)(1)) Important definitions Depending on availability, confidentiality, and integrity, the following terms are not explicitly defined in the security rule. The definitions in this Guideline, in line with the common sectoral definitions, put discussions on risk analysis in context. These expressions do not modify or update the security rule and cannot be interpreted as insensible to the terms used in the security rule. The vulnerability is determined by an error or weakness in NIST 800-30 nist, which can be practiced (inadvertently exploited) (inadvertently exploited) and that result in a violation or violation of the security policy of the system. Vulnerabilities, whether inadvertently activated or intentionally exploited, could cause a security incident, such as inappropriate access to or disclosure of e-PHI. Vulnerabilities fall into two general categories: technical and non-technical Categories. Non-technical vulnerabilities can be ineffective or non-existent policies, procedures, standards, or guidelines. Technical vulnerabilities can include holes, holes, shortcomings in the development of information systems; or incorrectly implemented and/or configured information systems. Threat An adapted definition of a threat from NIST SP 800-30 could potentially be for a person or something to practice (inadvertently trigger or intentionally exploit) a specific vulnerability. There are several types of threats that can occur on the information system or in the operating environment. Threats can be classified into general categories, such as natural, human and environmental. Examples of common threats in all of these general categories include: • Natural threats such as floods, earthquakes, tornadoes, and landslides. • Human threats are authorised or caused by humans and may include intentional (e.g. network and computer attacks, uploading of malicious software and unauthorized access to e-PHI) or unintentional (e.g. accidental entry or deletion and inaccurate data entry). • Environmental hazards such as power outages, pollution, chemicals and liquid leakage. Risk The adapted definition of nist sp 800-30 risk is as follows: The impact of the net mission taking into account (1) the likelihood that a given [threat] will exert a specific [vulnerability] (inadvertently triggers or intentionally exploits) a specific [vulnerability] and (2) the resulting impact if this occurs. [R]isks stem from legal liability or loss of mission- 1. Disclosure, modification or destruction of unauthorised information (malicious or accidental) 2. Unintentional errors and omissions 3. IT disruptions due to natural or man-made disasters 4. Failure to take due care and diligence in the implementation and operation of the IT system. The risk 1) the likelihood that a particular threat will trigger or exploit a specific vulnerability, and 2) the resulting impact on the organization. This means that the risk is not a single factor or event, but a combination of factors or events (threats and vulnerabilities) that can adversely affect your organization if they occur. Elements of risk analysis There are many methods of risk analysis and there is no single method or best practice to ensure compliance with the safety rule. For some examples of steps that can be used in the risk analysis process, see NIST SP 800-30.6. Scope of analysis The risk analysis, which is covered by the security rule, shall include the potential risks and vulnerabilities of the confidentiality, availability and integrity of the e-PHI created, received, maintained or transmitted by the organisation. (45 C.F.R. § 164.306 (a).) This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, DVDs, DVDs, smart cards or other storage devices, personal digital transfer media or portable electronic media. Electronic media media workstation and complex networks connected between multiple places. Thus, the risk analysis of the organization should take into account all of its e-PHI, regardless of whether it is on the specific electronic medium in which it was created, received, maintained or transmitted, or the source or location of the e-PHI. Data collection The organisation shall determine where e-PHI is stored, received, maintained or transmitted. An organization can collect relevant data by reviewing past and/or existing projects; carrying out interviews; review of the dossier; or other data collection techniques. Data on e-PHI collected by these methods shall be documented. (See § 45 C.F.R. § 164.308(1) (ii)(A) and 164.316(b)(1)) Identify and document potential threats and vulnerabilities Organizations should identify and document reasonably expected threats to e-PHI. (See § 45 C.F.R. § 164.306(a) (2) and 164.316(b)(1)(ii)) Organizations can identify different threats unique to the circumstances of their environment. Organizations should also identify and document vulnerabilities that may cause inappropriate access to or disclosure of e-PHI in the event of a threat or exploitation. (See § 45 C.F.R. § 164.308(1) (ii)(A) and 164.316(b)(1)(ii))) Assessment of current security measures Organizations should evaluate and document the security measures that the entity uses to protect e-PHI, whether the security measures required by the security rule are already in place, and whether the current security measures are properly configured and used. (See § 45 C.F.R. § 164.306(b)(1), 164.308(1) (ii) (A) and 164.316(b)(1)) Security measures implemented to reduce risks may vary from organisation to organisation. For example, small organizations tend to have more control within their environment. Small organisations usually take into account fewer variables (i.e. fewer workforce members and information systems) when making decisions on the protection of e-PHI. As a result, appropriate security measures that reduce the confidentiality, availability, and integrity of e-PHI in a small organization may differ from appropriate security measures in large organizations.7 Determine the likelihood of compromise. (See 45 C.F.R. § 164.306 b) 2. (iv) The results of this assessment, together with the initial list of threats, influence the determination of what threats the rule requires protection against because they are reasonably foreseen. The output of this part should document all threat and vulnerability combinations and related probability estimates which may affect the confidentiality, availability and integrity of the organisation's e-PHI. (See § 45 C.F.R. § 164.306(b)(2) (iv),164.308(a) (1)(ii)(A) and 164.316(b)(1)(ii)) Determine the potential impact of threat occurrence The rule also requires you to consider criticality, criticality, potential risks to confidentiality, integrity and e-PHI availability. (See 45 C.F.R. § 164.306 b) 2. (iv) Your organization should assess the magnitude of the potential impact of a threat that could trigger or exploit a specific vulnerability. An entity may also use a qualitative or quantitative method or a combination of the two methods to measure the impact on the entity. The output of this process should be to document all potential impacts related to the occurrence of threats that trigger or exploit vulnerabilities that affect the confidentiality, availability, and integrity of e-PHI within the organization. (See § 45 C.F.R. §§ 164.306(a) (2), 164.308(1) (ii) (A) and 164.316(b)(1)(ii))) To determine the risk level organizations must assign risk levels to all threat and vulnerability combinations identified during risk analysis. The level of risk can be determined, for example by analyzing the values assigned to the likelihood of a threat occurring and the resulting impact of the threat occurrence. The risk level can be determined by attributing a risk level based on the average of the assigned probability and impact levels. The issue shall be a documentation of the assigned risk levels and a list of corrective measures to be taken to reduce each risk level. (See 45 C.F.R. §§ 164.306 a) (2), 164.308(1) (ii) (A) and 164.316(b)(1)) Finalization of documentation The security rule requires risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316 b) 1.Risk analysis documentation shall be a direct contribution to the risk management process. Periodic review and updating of the risk assessment The risk analysis process should be continuous. In order for an entity to update and document the security measures required by the rule as needed, you must perform a continuous risk analysis to determine when updates are required. (§ 45 C.F.R. § 164.306(e) and 164.316(b)(2)(iii)) The security rule does not specify how often you perform risk analysis as part of a comprehensive risk management process. The frequency of performance varies between the affected organizations. Some organisations concerned may carry out these processes annually or as necessary (e.g. every six months or every three years), depending on the circumstances of their environment. New technologies and business operations implement a planned, truly integrated risk analysis and management process, thereby reducing the efforts needed to manage the risks identified after implementation. For example, if the organisation concerned has experienced a security incident, has experienced a change of ownership, the turnover of key personnel or management, plans to incorporate new technology to make operations more efficient, the potential risk should be analysed in order to to ensure that e-PHI is reasonably and adequately protected. If it is found that existing security measures are not sufficient to the introduction of a changing business environment or new technology, the entity shall determine whether additional security measures are necessary. Carrying out a risk analysis and adjusting risk management processes appropriately to manage risks in a timely manner will allow the entity concerned to reduce the associated risks to a reasonable and appropriate level.8 In the summary risk analysis, the first step in the organisation's compliance efforts with security rules. Risk analysis is an ongoing process that needs to understand in detail the risks to the confidentiality, integrity, and availability of e-PHI for the organization. Resources Documents on the Civil Rights Office (OCR) website ( available security series include a more detailed encyclical on the tools and methods available for risk analysis and risk management, as well as other compliance requirements for safety rules. Visit our for the latest guidance, FAQs and other information about the security rule. A number of other federal and non-federal organizations have developed materials that may be useful to the scope of organizations designed to develop and implement risk analysis and risk management strategies. The Department of Health and Human Services does not support or recommend any specific risk analysis or risk management model. The documents referred to below do not constitute legally binding guidance for the organisations concerned, nor does compliance with any or all of the standards contained in these substances demonstrate that they substantially comply with the risk analysis requirements of the safety rule. Rather, materials are examples of frameworks and methods that some organizations use to guide their risk analysis efforts. The U.S. Department of Commerce's Office, the National Institute of Standards and Technology (NIST), is responsible for developing information security standards for federal agencies. NIST has produced a publications that provide information relevant to the security of information technology. These documents include: Guidance on the technical aspects of carrying out information security assessments (SP800-115) Information Security Manual: Guidance for Managers (SP800-100; Chapter 100; chapter contains a risk management framework and details the steps in the risk management process) Introductory Resource Guide to implementing the Health Insurance Portability and Accountability Act (HIPAA) Safety Rule (SP800-66); Part 3 links the components of the NIST risk management framework to the security In the draft publication, Risk Management Information Systems (SP800-39) the Office of the National Coordinator for Health Information Technology (ONC) prepared a risk assessment guide for small health practices, known as reassessment of security practices in a health IT environment. The Society of Health Information and Management Systems (HIMSS), (HIMSS), a consortium of health information technology stakeholders has set up an IT security practice consultation. The questionnaire was created to gather information on IT security in the health sector, but it can also be a useful self-assessment tool in the risk analysis process. The Health Information Trust Alliance (HITRUST) has worked with industry to establish the Common Security Framework (CSF), a protected resource that . The risk management section of the document, Control Name: 03.0, describes the role of risk assessment and management in the overall development and implementation of security programmes. The document describes the methods of implementation of the risk analysis programme, including requirements for knowledge and processes, and links the different existing frameworks and standards to the applicable points in the information security lifecycle. Final remarks [1] Section 13401(c) of the Health Information Technology Economic and Clinical (HITECH) Act[2] As used in the Guide, the term organizations refers to the organisations and associates concerned. The guidelines will be updated following the implementation of the hitech final regulations. [3] HIPAA Security Rule: Health Insurance Reform: Safety Standards, 2003.[4] 800 Series Special Publications (SP) are available on the Office of Civil Liberties website – specifically SP 800-30 – Risk Management Guide for IT Systems. ( [5] See NIST SP 800-66, When applying the HIPAA #4 section. Available [6] Available . [7] For more information about the methods used by smaller organizations to achieve compliance with the security rule, see #7 in the Center for Medicare and Medicaid Services (CMS) Security Series Implementation for the Small Provider. Available in . [8] For more information about the methods used by smaller organizations to achieve compliance with the security rule, see #6 Center for Medicare and Medicaid Services CmS) Security Series, titled The Basics of Risk Analysis and Risk Management. Available in . The content produced by the Office of Civil Rights (OCR) last reviewed office's 22 July 2019.