1. Purpose – To regularly identify, rate, and document risks to the information systems that store, process, transmit, or receive electronic Protected Health Information (ePHI).

2. Risk Analysis Policy – Boston University’s Covered Entities (CEs), under the direction and with the assistance of the Information Services & Technology (IS&T) Information Security group, must implement a formal, documented risk analysis process to identify, rate, and document risks to the information systems that handle ePHI. A review and update of the CEs’ risk analyses will be performed annually and whenever environmental or operational changes occur that may affect the confidentiality, integrity, or availability of ePHI.

2.1. At a minimum, the CEs’ risk analysis process must include the following:

2.1.1. Identification, documentation, and classification of the threats to information assets containing ePHI.

2.1.2. Identification, documentation, and classification of the vulnerabilities of information assets containing ePHI.

2.1.3. Identification of security safeguards (procedures and controls) used to protect the confidentiality, integrity, and availability of ePHI.

2.1.4. Estimation of the likelihood that a given threat will exploit a specific vulnerability on a system containing ePHI.

2.1.5. Identification of the potential impacts to the confidentiality, integrity, and availability of information systems containing ePHI if a given threat exploits a specific vulnerability.

2.1.6. Qualitative estimates, assumptions, and uncertainties.

2.2. The risk analyses should be integrated with the CE’s risk management process so that appropriate safeguards can be selected and implemented to protect the confidentiality, integrity, and availability of ePHI. See Risk Management Policy [BU 000-001B].
BOSTON UNIVERSITY

2.3. In addition to periodic risk analysis, CEs must conduct a risk analysis when environmental or operational changes occur that might affect the confidentiality, integrity, or availability of ePHI. Such changes include, but are not limited to:

2.3.1. Significant security incidents
2.3.2. Significant new threats or risks to information assets
2.3.3. Significant changes to the organizational or technical infrastructures
2.3.4. Significant changes to information security requirements or responsibilities

3. Risk Analysis Procedure – For detailed risk analysis procedures, see chapter 3 of NIST Special Publication 800-30. A CE’s risk analysis process must be based on the following steps:

3.1. Inventory – Conduct a regular inventory of information systems that store, process, transmit, or receive ePHI and the security measures protecting those systems.

3.2. Threat identification – Document all potential threats (human, natural, and technical/environmental) to critical information and ePHI.

3.3. Vulnerability assessment – Identify and document known vulnerabilities in information systems that handle ePHI. This should be done regularly by reviewing vulnerability information sources (e.g. web sites), scanning, and performing security assessments.

3.4. Security control assessment – Gauge the effectiveness of existing safeguards that protect ePHI. Include both preventive and detective controls.

3.5. Risk likelihood determination – Assign values to specific risks that indicate the probability that a particular vulnerability will be exploited by a particular threat. Three factors should be considered: threat motivation and capability, type and extent of vulnerability, and effectiveness of current security controls.

3.6. Impact analysis - Estimate the impact to confidentiality, integrity or availability of ePHI and critical systems that would result if a threat were to successfully exploit one or more of the identified vulnerabilities.

3.7. Risk Determination - Use the information obtained in the steps above to document the level of risk to each information system that stores, processes, transmits, or receives ePHI. For each vulnerability and associated threat, make a risk determination based on:

3.7.1. The likelihood that a certain threat will attempt to exploit a specific vulnerability.
3.7.2. The level of impact that could result from the exploit of the vulnerability.
3.7.3. The effectiveness of planned or existing security controls.

3.8. The results of each of the above steps must be formally documented and retained for six years.