The final Health Insurance Portability and Accessibility Act (HIPAA) security regulations were released in February (Federal Register 68:8334-8381; downloadable at www.cms.gov). They apply to protected health information in electronic form (E PHI). Enforcement will begin April 2005. The final rule requires that covered entities determine appropriate security measures through risk analysis, adjust security practices as circumstances change, and revisit the security needs associated with "appropriate administrative, technical and physical safeguards" for protected information implemented under the privacy regulations.

Approaches to risk analysis

According to the final rule, risk analysis is a thorough assessment of potential risks to the confidentiality, availability and integrity of E PHI. Vulnerabilities of E PHI must be identified and the effects of potential threats calculated as if they actually occurred. If potential threats create an unacceptable risk, safeguards are to be implemented. The rule doesn't require a certain risk-analysis approach, but the following are well accepted.

- **Quantitative analysis:** Measure and assign objective numeric value to assets, potential threat impacts, safeguard effectiveness, safeguard costs, uncertainty and probability; a tedious process not often followed in its purest form
- **Qualitative analysis:** Ascribe relative rank to threats and vulnerability of assets according to seriousness, then match potential level of threat to potential asset loss to select appropriate safeguard; sometimes imprecise but helpful in prioritizing risks

Each method has strengths and weaknesses. A quantitative approach provides a more workable cost/benefit analysis but requires extensive study for asset valuation and threat probability. A qualitative approach is relatively simple but depends largely on subjective information.
Seven steps

The following basic steps should be considered when conducting risk analysis.

1. Conduct a complete inventory to determine assets needing protection; use the following list as a starting point to identify where EPHI is received, stored and transmitted, and who has access to it:

- Hardware--computers, radiology storage devices, medical equipment, front-end processors, workstations, modems
- Information networks--servers, communication lines, internal and external connectivity, remote access
- Applications--database and application software, operating systems, utilities, compilers, encryption tools, procedure libraries
- Physical facilities--heating, ventilation and cooling systems; furniture; supplies; machinery; fire control systems; storage
- Other assets--records and data, policies and procedures, customer confidence

2. Determine the value of every asset. For example, use financial statements to value physical assets. With EPHI, one method is to consider the cost of creation and protection, attributable revenues, competitive advantages provided and value to third parties. Initial creation and valuation of an asset inventory can be tedious, but it will be helpful, for example, in contingency and risk-insurance planning.

3. Identify vulnerabilities and threats for each asset. A vulnerability is a software, hardware, or organizational weakness that may allow unauthorized access. A threat is any potential danger to the information system that exploits that vulnerability. For example, software code that permits system access without a password is a vulnerability. Someone accessing the system to steal or destroy stored information is a threat. Some vulnerabilities can pose more than one threat, so risk analysis must be thorough.

4. Evaluate the impact, or severity, of each threat for every asset in the inventory. For quantitative analysis, first determine the exposure factor (EF)--the percentage of loss a threat would likely cause the asset and the EPHI connected with it. For example, if a fire in the computer server room could be expected to destroy half of the servers, the fire threat is 50 percent. Using the EF, determine the single-loss expectancy (SLE)--the effect of a single occurrence of the threat for each asset and its EPHI. If the EF is 50 percent and the servers and their EPHI are worth $3 million, the SLE from a fire is $1.5 million. The SLE is used in cost/benefit analysis for selecting safeguards.

For qualitative analysis, rate the impact on a scale, such as 0 for none and 5 for severe. In the fire example, impact might be valued at 3 if the organization could function after losing half its servers. If the servers contain all the information needed to function, the rating would be 5.
5. Determine the probability of a threat. For quantitative analysis, establish the annualized rate of occurrence (ARO). In the example, fire-occurrence averages compiled by local insurance companies could be used. Say statistics show there's a server room fire once every five years. The ARO would be one-fifth, or 20 percent. For qualitative analysis, the probability of a fire might be, based on the consensus of management and the risk-analysis team, given a 1.

6. Calculate the annual expected loss or total risk level for a threat. For quantitative analysis, the amount lost or paid out if the threat occurs is determined by multiplying the SLE (step 4) by the ARO (step 5). The organization experiencing the fire could expect to lose $300,000 annually ($1.5 million x 20 percent).

For qualitative analysis, determine total risk by multiplying the threat's impact by its probability. Since a 5-point scale was used for each in the example, total risk is measured on a 25-point scale. Impact (5) x probability (1) = total risk of 5, a relatively low score on a 25-point scale.

7. Identify safeguards for each vulnerability—those currently used and those addressable or required by HIPAA (e.g., a fire suppression unit in the server room). For quantitative analysis, measure the cost of purchasing, installing and maintaining each safeguard against the cost of a threat occurrence. With a fire costing $300,000, a $50,000 fire suppression unit is well worth the price. For qualitative analysis, the cost of each safeguard is important even though exact expense calculations aren't required. For example, spending $200,000 to counter a low-probability risk makes little sense.

**Transferring or accepting risk**

When eliminating or mitigating risk to an acceptable level is impossible, one option is to transfer it, which is usually accomplished by purchasing insurance. More insurance companies are beginning to offer cyber insurance, but policies seldom cover fines and cannot restore good will lost during a security incident.

Another option is to accept a technical risk that is unlikely to occur—after full disclosure of this intention to legal, risk management and executive personnel and the board of directors. But even with transfer or acceptance of risk, the security regulations require some form of risk analysis.

---

*M. Peter Adler, J.D., CISSP, is a partner in the health law department of Foley & Lardner, Washington, D.C.*