

“Reasonable Threats”

In today’s world, just what could be considered a “reasonable” threat? The HIPAA Security rule §164.306(a)(2) directs a covered entity to “Protect against any reasonably anticipated threats or hazards to the security or integrity of such information (electronic protected health information the covered entity creates, receives, maintains, or transmits).

The preamble (page 8346) further provides insight into this issue when it quotes “NIST SP 800-30, “Risk Management guide for Information Technology Systems, Chapters 3 and 4, January 2002. An entity must identify the risks to and vulnerabilities of the information in its care before it can take effective steps to eliminate or minimize those risks and vulnerabilities.”

So, in order to work through your HIPAA Security implementation risk analysis process (see previous TIP), you must carefully consider threats to the ePHI your organization creates, receives, and works with in general.

This month’s Security E-TIP will explore two areas for your use when conducting this process.

1. Even though the Security rule is dealing with “electronic protected health information” EPHI, there are many natural, environmental and man-made threats which could compromise the integrity of your ePHI. Consider your demographic location...if your facility is located in an area susceptible to flooding, have you taken measures to best protect your ePHI and the systems and buildings where it is housed? Have you beefed up your business continuity (disaster planning) processes in consideration of a potential flood? PCI/Clayton Group has provided a handy one page chart for your use when considering reasonable threats. Be sure to “grade” such threats that are possible in your environment by assigning a “high, medium or low” grade based upon the potential for it to occur and its impact upon your organization if it should occur. NOTE: This is not an all inclusive list, it should be customized for your organization and is best suited for a smaller environment. A more complex environment should consider expanding such process and use NIST or other nationally recommended guidelines as a reference.
2. In regard to protecting one’s ePHI in the “virtual” environment (as opposed to the physical environment) from such threats as:
 - Hackers
 - Data integrity/destruction issues
 - Malicious code (viruses, spyware, bad patches, etc.)
 - Misuse of resources

one can refer to the following five elements to provide guidance in taking reasonable precautions against these aforementioned threats.

Authorization refers to any means of limiting access to resources. Authorization answers the questions of, “Who has access to the network?”, “From where can access be achieved?”, and “How is this access granted?”. Authorization generally addresses the areas of access policy creation, authentication (single-factor vs. multiple-factor), and remote accessibility of resources.

Encryption should be used whenever it is reasonable to do so. If transmitting any ePHI over the Internet or other public avenues, encryption should be considered a mandatory practice. Many organizations even elect to encrypt data on storage devices, so as to mitigate risk in the event that said storage medium might be lost or stolen. Encryption within one's network can also prevent theft of sensitive data from inside sources.

Installation can include anything from the types of technology used to the manner in which they are deployed. Installation of insecure or rogue wireless access points can leave a network vulnerable to "war drivers" – hackers who use wireless sniffing technologies to steal bandwidth and data. An unlocked server room is susceptible to physical theft of or damage to critical resources. Even poorly positioned or unshielded monitors allow wandering eyes to recover data directly from the screen itself. These are just a few examples illustrating the importance of a sound network installation.

Operation and Utilization refer to how one's resources are (and are not) to be used. Wherein authorization determines if a user can access the network, operation and utilization focus on what a user can access on the network. Productivity is another focus under the umbrella of operation and utilization. Are potential time- and bandwidth-wasters such as games and/or streaming media allowed within the network? Does one's organization have the technology to enforce an acceptable usage policy for Internet surfing? Does the network administrator have the ability to monitor what programs can be downloaded/installed on the network? The bottom line with operation and utilization is to have knowledge and control of what one's users can do within the network.

Only by utilizing an implementation/administration strategy that takes into consideration these focus areas can an appropriate level of security awareness can be achieved. As in the previous step, one should "grade" their environment so as to ascertain how one's network rates against potential threats. In better knowing what possible risks one's network is exposed to, one may then take the necessary – if reasonable – steps to safeguard against said threats.



POTENTIAL THREATS WORKSHEET

Threat Natural, Human, Environmental (Reference 164.308 a 1 A)	Likelihood of Occurrence & Impact Not Applicable, Low, Medium, High
Cold, frost and snow	
Earthquakes	
Errors (human)	
Explosion Bomb threat	
Fire Fire alarm	
Flooding and water damage	
Fraud	
Hackers Data integrity Data destruction	
Hardware Failure	
Hazardous material incident Chemical contamination	
Malicious software (i.e. viruses)	
Public Utility Failure (electrical, etc.) Air conditioning Communications Loss Other power loss	
Radiological incident (seepage, spills)	
Sabotage Blackmail Fraud/embezzlement Vandalism/rioting	
Sinkhole	
Storms and Hurricanes	
Theft Of data, Of assets	
Vandalism	
Workforce issues Errors, Misuse of computer time Misuse of resources	
Other	