



## HIPAA – A Reasonable Piece of Legislation

Health care related organizations throughout the United States are trying to understand what the *Health Insurance Portability and Accountability Act (HIPAA) of 1996* means to them. The legislation itself is actually very reasonable. In fact, it is the *reasonableness* of the act that makes it so difficult to understand!

HIPAA requires that organizations take “reasonable” steps to ensure the security and privacy of health care information. Unfortunately, this is a highly subjective standard. Some have suggested that *reasonable* measures are those taken by a *prudent* person. In our opinion this is not very helpful since it simply substitutes one unverifiable word for another.

Since it is cost prohibitive to plug every conceivable chink in our information security armour, the question remains, “Which risks will require mitigation in order to meet HIPAA standards?” Until HIPAA is tested in court, no one can be absolutely certain how the legislation will be interpreted. However, **health care providers that implement solutions based on the objective, methodical analysis provided by Secur/Tree® should have an advantage in demonstrating “due diligence” over security schemes founded on subjective lines of reasoning.**

Even if it were possible to identify and create a mitigation plan for every information related vulnerability, the cost would be horrendous. Significantly higher health care premiums would result. Neither patients nor health care providers benefit from million dollar tonsillectomies! **Secur/Tree allows you to systematically determine the optimal level of risk where the privacy of the patients’ is protected in a cost effective fashion.**

Amenaza Technologies Limited embraces and promotes an analytic technique known as *Attack Tree Analysis*. Using Amenaza’s risk analysis tool, Secur/Tree, a model is created of all possible attacks on your information systems. By applying attack tree analysis to the model, all (reasonably) impossible attacks are removed. **The remaining attacks, displayed in an easy to understand graphical format, are those that “a prudent person” would address.**

A Secur/Tree model automatically documents all of the vulnerabilities and threats that were considered at the time of analysis, as well as the reasoning used to eliminate unlikely attacks. Wouldn’t you rather defend your actions with this information clearly documented rather than relying on conflicting and uncertain memories?

Lord Rothschild once said, “There is no point in getting into a panic about the risks of life until you have compared the risks that worry you with those that don’t, but perhaps should.” This, in essence, is the philosophy behind the Secur/Tree attack tree-based methodology. **By demonstrating that your organization has methodically and systematically determined which threats must be addressed and which may be ignored, you can comply with HIPAA while controlling costs.**



**Secur/Tree® – Dare you risk IT?**



# Amenaza

TECHNOLOGIES LIMITED

*Amenaza Technologies Limited has developed the world's most advanced Attack Tree based vulnerability assessment tool, SecurITree®. When used with the accompanying methodology and attack tree libraries, SecurITree allows enterprises to discover which weaknesses are most likely to be used against them by attackers. SecurITree turns the tables on the attackers by enabling enterprises to quickly and efficiently invest in those security measures that result in the greatest reduction of risk.*

*Learn more about Amenaza Technologies and SecurITree at [www.amenaza.com](http://www.amenaza.com)*

