Clinical Notes

security: a new clinical engineering paradigm

Stephen L. Grimes

Security is the new mantra. Particularly since the tragic events of 9/11, the world has become preoccupied with security. The United States creates a cabinet post and a new mega entity called the Department of Homeland Security. The resources of a countless number of government, public, and private organizations are now focused on security issues. Security topics are addressed regularly on television and in nearly every conceivable type of magazine, newspaper, journal, and conference. Security-related businesses and consultants seem to be proliferating and permeating every aspect of our business and personal lives.

The world's preoccupation with security seems justified when we are continually confronted with sobering reports as to our vulnerability to attack. There are reported threats involving the use of weapons of mass destruction, attacks to or involving the use of our transportation systems (e.g., air, rail, ship, and truck), biocontamination of our water supplies and mail, and cyber attacks to our information systems.

The healthcare system is not immune to the variety of threats that exist. Clinical engineers are increasingly being called on to address the security vulnerabilities of medical technology that has become integral to the delivery of care. The need to address these security issues requires that clinical engineers adopt what will be for most a new paradigm. That paradigm, as it turns out, effectively addresses not only threats associated with malfeasant acts but any threat or risk that would compromise the efficacy or availability of the medical technology that clinical engineers typically manage.

The New Paradigm

Rather than focusing on the management of discrete devices as has been the practice of traditional clinical engineering services, the new "security" paradigm requires adoption of a security process that includes the following:

1) identifying and rating the technology systems in terms of criticality of the information these systems maintain or transmit (i.e., information acquired through diagnostic systems or acted on by therapeutic systems)
2) determining vulnerabilities the information is subject to and the probability of information compromise for each identified vulnerability
3) identifying existing security measures in place to protect (e.g., reduce the vulnerability of) information and any additional measures that would be necessary to achieve an acceptable level of risk
4) developing a mitigation plan to implement additional security measures and establishing plan priorities based on information criticality and the probability of compromise
5) testing and monitoring the effectiveness of the security process and modifying the process to improve that effectiveness as necessary.

Note that the emphasis in the security process is on *information*. Medical devices must acquire, process, and/or act on information. Information is the "blood" sustaining the "body" that is the healthcare process. Medical technology serves as the vessel for that information.

Clinical engineers need to develop an understanding of the security process and how that process must be applied to preserve the *integrity, availability,* and *confidentiality* of information. Failure to safeguard information leads to the malfunction of medical technology and the breakdown of that portion of the healthcare process that medical technology supports. The consequences to the patient of this breakdown can range from injury to inappropriate or delayed treatment to the loss of privacy. Conversely, an effective security process that successfully safeguards the integrity, availability, and confidentiality of information can insure that medical technology is available and applied in a manner that supports the timely and effective delivery of quality healthcare.

Some of the more common threats to the integrity, availability, and confidentiality of information maintained or transmitted by medical technology include:

- data accessed or modified (i.e., tampering) by unauthorized personnel or processes (locally or remotely), including computer viruses and worms
- device or component failure
- device/system errors (e.g., "out of calibration")
- device/system user misuse/abuse
- electromagnetic interference (EMI) or other adverse environmental effects
- erroneous data input (by processes or personnel)
- interruption of required utilities (e.g., power outage), services, or supplies
- physical assault (e.g., fire, flood, theft, vandalism, accident)
- procedural violations by device/system users.

Once identified, threats must be evaluated as to their criticality and probability. Based on that evaluation, the clinical engineer needs to develop a plan where priority is given to mitigating the most critical and most probable threats. Examples of safeguards to consider in the mitigation process include:

- antivirus software with regular updates

(continued on page 82)

Strategic Health Care Technology Associates

Stephen L. Grimes, FACCE
Senior Consultant & Analyst

139 Henry Street
Saratoga Springs, NY 12886

Phone 518.441.5617
Fax 360.234.8894
slgrimes@nycap.rr.com

Clincal Notes *(continued from page 80)*

- device operating environment with appropriate physical safeguards (e.g., maintaining environmental conditions and incorporating appropriate protection against potential physical damage or loss)
- inventory of replacement components (to effect repairs) and devices (to provide backup systems)
- operating areas for device/system that are only accessible to and/or viewable by authorized personnel and patients
- physical safeguards and alarms integrated with the device/system
- policy/procedure restricting or controlling use of EMI-generating devices in areas where this device is operated
- processes to insure timely updating, upgrading, or replacement of biomedical devices/systems, which includes consideration of security issues
- a program that insures adequate scheduled maintenance and calibration of the device/system
- a program that insures security updates for device operating system are current
- routine data backups (with backups stored in secure and accessible locations)
- secure data so as to be accessible to only authorized personnel (e.g., encryption, secure private networks, virtual private networks, firewalls, lock and key, password, biometrics)
- secure operating controls so as to be accessible to only authorized personnel (e.g., lock/key, passwords, biometrics)
- user education on measures necessary to prevent, detect, and address data (integrity, availability, confidentiality) problems associated with device/system

After applying appropriate safeguards, clinical engineering needs to test and monitor the security process, modifying it as necessary to improve its effectiveness.

Conclusion

Security has become a universal concern. It is time for clinical engineering to get up to speed and recognize the benefit an effective security process can bring to medical technology management. The security paradigm appropriately focuses on insuring the integrity, availability, and confidentiality of information maintained and transmitted by medical devices rather than on the management of discrete devices. It is worthwhile noting that this process will soon be *required* for US healthcare providers. The U.S. Department of Health and Human Services has established a Security Rule [1] (part of the Health Insurance Portability and Accountability Act's Administrative Provisions), which will require the adoption of such a security process by 21 April 2005.

References

[1] U.S. Department of Health and Human Services, "Security standards; Final rule," *Federal Register*, vol. 68, no. 34, 45 CFR Pts. 160, 162, and 164, Feb. 20, 2003. [Online]. Available: http://www.cms.hhs.gov/hipaa/hipaa2/ regulations/security/03-3877.pdf