[Environmental Health and Preventive Medicine 10, 282–285, September 2005]

Special Issue

Commentary

Strategic Approach to Information Security and Assurance in Health Research

Shunichi AKAZAWA[1], Manabu IGARASHI[2], Hirofumi SAWA[3] and Hiko TAMASHIRO[2]

[1]*Kyoto University Graduate School of Medicine & World Health Organization (WHO) Headquarters*
[2]*Hokkaido University Graduate School of Medicine*
[3]*Hokkaido University Research Center for Zoonosis Control*

Abstract

Information security and assurance are an increasingly critical issue in health research. Whether health research be in genetics, new drugs, disease outbreaks, biochemistry, or effects of radiation, it deals with information that is highly sensitive and which could be targeted by rogue individuals or groups, corporations, national intelligence agencies, or terrorists, looking for financial, social, or political gains. The advents of the Internet and advances in recent information technologies have also dramatically increased opportunities for attackers to exploit sensitive and valuable information.

Government agencies have deployed legislative measures to protect the privacy of health information and developed information security guidelines for epidemiological studies. However, risks are grossly underestimated and little effort has been made to strategically and comprehensively protect health research information by institutions, governments and international communities.

There is a need to enforce a set of proactive measures to protect health research information locally and globally. Such measures should be deployed at all levels but will be successful only if research communities collaborate actively, governments enforce appropriate legislative measures at national level, and the international community develops quality standards, concluding treaties if necessary, at the global level.

Proactive measures for the best information security and assurance would be achieved through rigorous management process with a cycle of "plan, do, check, and act". Each health research entity, such as hospitals, universities, institutions, or laboratories, should implement this cycle and establish an authoritative security and assurance organization, program and plan coordinated by a designated *Chief Security Officer* who will ensure implementation of the above process, putting appropriate security controls in place, with key focus areas such as *policies and best practices*, *enforcement and certification*, *risk assessment and audit*, *monitoring and incident response*, *awareness and training*, *and modern protection method and architecture*. Governments should enforce a comprehensive scheme, and international health research communities should adopt standardized innovative methods and approaches.

Key words: security and assurance, health research information, proactive measures, ISMS, CSO/CISO

Risks involved in health research information

Information security and assurance is an increasingly critical issue in health research. Health research deals with information that is highly sensitive, be it health care record of individuals/populations, genetic epidemiology, disease outbreak information of nations, or data on new drugs/bio-chemicals. They are targets for rogue individuals or groups, corporations, national intelligence agencies, or terrorists, looking for financial, social, or political gains. Insurance companies are eager to discover detailed medical histories of their customers and their customers' families to define the most cost effective insurance premiums. Corporations could recruit new staff, decide assignments, or select future executives, based on genetic profiles of

Received Jun. 1, 2005/Accepted Jul. 25, 2005
Reprint requests to: Hiko TAMASHIRO
Department of Health for Senior Citizens, Division of Preventive Medicine, Social Medicine Cluster, Hokkaido University Graduate School of Medicine, North 15 West 7, Kita-ku, Sapporo 060-8638, Japan
TEL: +81(11)706-5051, FAX: +81(11)706-7374
E-mail: tamashiro@med.hokudai.ac.jp

employees. Early disease outbreak news is extremely valuable to stock exchange traders and speculators, whereas terrorists and intelligence agencies may have political reasons to interfere with early outbreak alert and response operations. Alternatively, a mere unwarranted disclosure of outbreak information could have a profound impact on the economy of nations who depend on tourism. Web sites posted by health scientists describing the impact of new deadly bio-chemical or radiation materials could be a textbook for terrorists.

The advent of the Internet and advances in recent information technologies have revolutionalized the way health research is conducted, and have made it extremely efficient to collect, store, exchange and process vast amounts of scientific information, yet have dramatically increased opportunities for attackers to exploit sensitive and valuable information to their ends through sophisticated but rogue technological means. To make matters worse, research scientists tend to pay little attention to the security of their data. Laboratory systems are much less well protected than operation systems.

Current countermeasures and their problems

Some government agencies have deployed legislative measures to protect the privacy of health information, especially in the health care sector, and developed standard information security guidelines for epidemiological studies. However, the risks are grossly underestimated and little effort has been made to strategically and comprehensively protect the health research information of universities, hospitals, institutions, government agencies, and international communities, through adequate security management processes. There are hardly any health research centers in the world today, except those dealing with highly confidential military intelligence or counter-terrorism health data, for example, where an authoritative information security program has been established and implemented. Not to mention that these centers lacks institutionalized information security risk assessment processes. They have, simply, no idea what critical assets are there to protect, from who and why, when it comes to health research information.

There is a need to promote and enforce a set of proactive measures to strategically and comprehensively protect health research information both locally and globally. Such measures should be deployed at all levels, but will be successful only if research communities collaborate actively, supporting governments enforce legislative measures at a national level, and international community develops quality standards, concluding treaties if necessary, at the global level. International collaboration is necessary particularly to address security issues involved in unprecedented free flows of, and easy access to, scientific information across the Internet.

Strategic approach

The best proactive measure would be a rigorous security management process where a cycle of "plan, do, check, and act" is enforced (Fig. 1). The approach described is based on the British Standard Institute's BS7799-2:2002 (1), to be superseded by the International Standard Organization's ISO/

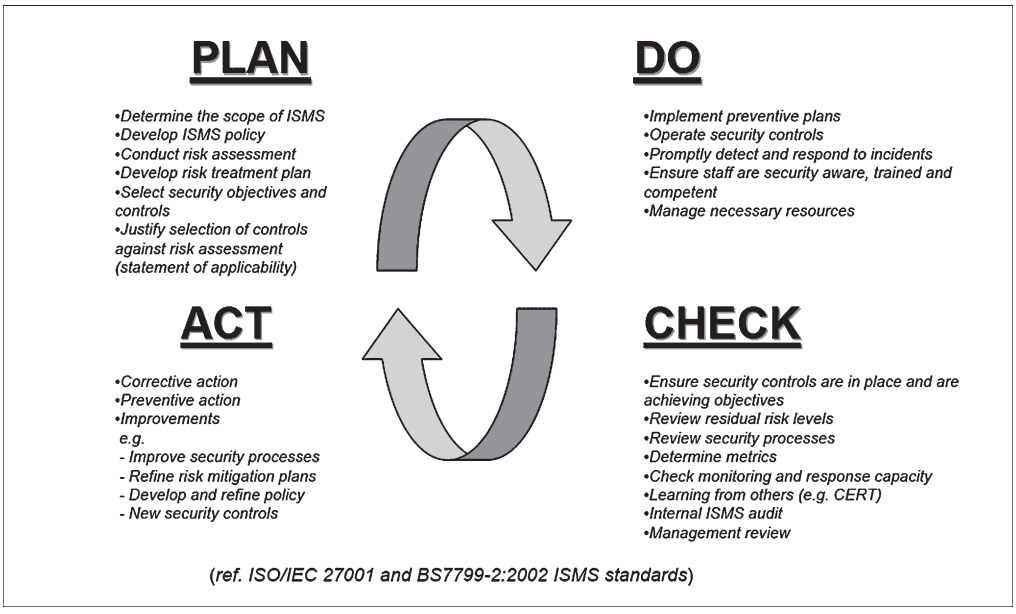

Fig. 1 Information Security Management System (ISMS) cycle.
Note: Information Security Controls and Best Practices are categorized by ISO/IEC17799:2005 (3) as: 1) security policy, 2) organization of information security, 3) asset management, 4) human resources security, 5) physical and environmental security, 6) communications and operations management, 7) access control, 8) information systems acquisition, development and maintenance, 9) information security incident management, 10) business continuity management, and 11) compliance.
Security control measures would include: 1) governance, technical and end-user policies; standards and reference architecture, 2) auditing and compliance assessment, certification, 3) vulnerability management, anti-malware (virus, worms, Trojan horses, SPAMS, spyware) systems, 4) access-control enforcement (firewalls/IPS (intrusion prevention systems), authentication, authorization, accounting systems, etc.), 5) monitoring, surveillance and response, incident response teams, and 6) awareness and training programs.

IEC27001. (ISO/IEC27001 for Information Security Management Systems (ISMS), could be considered one of the key quality assurance standards along with ISO9001 for Quality Management Systems (QMS), ISO14001 for Environment Management Systems (EMS), and OHSAS18001 for Health and Safety Management Systems (HSMS).)

The ISMS cycle consists of: the PLAN phase, where the ISMS's scope is defined, the ISMS's policy is developed, risk assessment is conducted, a risk management/risk treatment strategy is determined, security objectives and controls are selected, and selected controls are justified against risk assessment (i.e. statement of applicability (SOA)); the DO phase, where preventive plans are implemented, security controls are actually operated, and security incidents are promptly detected and responded to; the CHECK phase, where checks are made to ensure that security controls are firmly in place and are achieving goals, residual risk levels are reviewed, security processes are reviewed, metrics for evaluation are determined, monitoring and response capacity is checked, learning from others, such as CERT/CC (2), is done, an ISMS audit is conducted, and a management review is executed; and the ACT phase, where actions are taken to correct, prevent and improve (e.g. improvement of security processes, refinement of risk mitigation plans, development of new policies and refinement of existing policies, and design and implementation of new security controls).

Each health research entity, such as hospitals, universities, institutions, or laboratory centers, should implement this ISMS cycle, and establish an authoritative security and assurance management organization. Such an organization should be headed by a *Chief Security Officer* (CSO), or a *Chief Information Security Officer* (CISO), who takes charge of all information security and assurance issues and develops a security plan, coordinating the security program, ensuring the implementation of ISMS processes and manage/coordinates appropriate security controls, with key focus areas such as: *policies and best practices*, *enforcement and certification*, *risk assessment and audit*, *monitoring and incident response*, *awareness and training*, *and modern protection methods and architecture* (4). These six areas are particularly important because:

Policy and best practices: Policy describes exact rules and steps to be followed in order to improve security, whereas best practices are the behaviors which are considered to be effective by most industries, the public and experts, and followed often without formal assessment. Since security is not an exact science, both are needed.

Enforcement and certification: Policies and best practices are not effective unless they are enforced. Certification is to accredit officially and authoritatively compliance to policies, and is one of most effective methods of enforcement.

Risk assessment and audit: Risk is a multitude of [asset value]×[threat likelihood]×[threat impact]×[vulnerability], where critical assets could be tangible assets such as infrastructure—hardware and software, people, data, knowledge and services, or intangible assets such as privacy, reputation, credibility and absence of legal liability. Risks are moving targets, which change in time. Risk assessment is a key to understanding the current state of security at an organization, and should be conducted regularly. Audit verifies the successful implementation of security controls.

Monitoring and incident response: In security, prevention, detection, and response are all necessary. Most information security is preventive in nature, which is a countermeasure to provide two things: a) a barrier to overcome and b) time to overcome the barrier. Without detection and response, however, the preventive countermeasure is much less effective. In security, detection and response are often more effective, and more cost effective than more prevention (5).

Awareness and training: In security, "awareness and training" is critically important. After all, security is people-related: it is said that 70% of security problems are attributed to humans (people, process, and politics & culture). Without a security conscious and educated staff, many security measures, or much security technology, could be useless. Social engineering and taking advantage of human errors/negligence, continues to be one of the most effective attacks against information networks.

Modern protection methods and architecture: Although it is said that only 30% of security problems is related to technology, that 30% could still be significant. Choices and the adoption of appropriate modern and innovative protection technology methods and architecture, based on international and industry "best practices" and standards, could improve security substantially.

Only through such an authoritative and comprehensive program, could the information security and assurance of highly sensitive health research information be systematically and successfully protected from increasing threats and risks in the modern world.

To ensure that this strategic approach prevails, governments should enforce the scheme throughout all their agencies, and international health research communities should conclude a formal agreement to adopt standard methods and approaches. There already exist in the world a vast amount of scientific health research information not properly protected and in danger, and we must take action promptly to protect it from misuse, modification, loss/destruction, or unwarranted disclosure.

e-Health is becoming prevalent around the world, from highly sophisticated hospital information systems to Internet health portals, to telemedicine helping the poorest of countries or regions. Information security and assurance issues should seriously be addressed in e-Health (6). There are emerging communication applications on the Internet such as networked virtual offices for scientists to collaborate globally, ubiquitous RFID-based sensors to collect health data over wide areas, internationally federated identity management systems between collaborating research centers, and unimaginably powerful search engines which provide keys to almost any information people, or terrorists, are looking for. These new applications and the tremendous depository of digital information being accumulated and processed will force us to take coordinated efforts to push for a strategic approach to protecting health research information on a global scale.

Conclusion

This paper proposes a formal and comprehensive approach to protection of the security and assurance of health research information. Health research information has a high level of security requirements for: 1) confidentiality, 2) business continuity, 3) integrity, 4) quality, 5) availability, 6) authenticity, 7) accountability, 8) confidence, 9) credibility, and 10) absence of legal liability.

We believe that the approach described herein addresses collectively these issues and requirements, and facilitates a step forward toward a proactive global security process for the health research community.

Special note from authors: This paper solely reflects the views of the authors. It does not necessarily reflect the "official" views of the organization, WHO, or institutions they belong to.

References

(1) British Standard Institute. BS7799-2:2002 Information Security Management Systems—Specification with Guidance for Use, ISBN 0-580-40250-9: September 2002 (To be superseded by ISO/IEC27001, November 2005).
(2) Carnegie Mellon University Software Engineering Institute, Computer Emergency Response Team/Coordination Center (CERT/CC). Available at URL: http://www.cert.org/
(3) International Standard Institute. ISO/IEC17799: 2005: Information Technology—Code of Practices for Information Security Management: 2005.
(4) World Health Organization. WHO Global Information Security Policy and Implementing Guidelines: 2005.
(5) Schneier B. Managed Security Monitoring: Network Security for the 21st Century: Available at URL: http://www.counterpane.com/msm.pdf
(6) Akazawa Y, Akazawa S. WHO Strategy on 'e-Health' (and Information Security), Global Burdon of Impaired Glucose Tolerance—Present and Future Strategy. Nihon Rinsho. 2005; 63:600–602.