

# Stakeholder Analysis

## HIMSS Medical Device Security Work Group Security in Medical Devices Issue

### Document Background:

One of the agreed action items of the HIMSS Medical Device Security Workgroup is to: Coordinate with similar groups and committees, in HIMSS and other organizations, to capitalize on existing efforts and realize the economies of collaboration.

This discussion document is background information for this coordination and collaboration effort. It contains several tables that address aspects imbedded in the discussion about security in medical devices.

1. There is numerous security related legislation that impacts security in medical devices. (Table 1)
2. There are numerous national and international standards that impact security in medical devices. (Table 2)
3. There are many healthcare industry specific accreditation organizations that may impact or address the security in medical devices issue (Table 3).
4. There are many stakeholder organizations that are attempting to raise the awareness about the security in medical devices issues (Table 4). There are four very specific stakeholder audiences
  - A. Healthcare Professional, including providers and payors
  - B. Information Security Professionals
  - C. Consumers/Users/Patients
  - D. Government Regulators
  - E. Manufacturers

Ideally, as the discussion around solutions to the problems inherent in the security medical devices issue progresses among the various stakeholder groups, the list of applicable legislation, national and international standards, healthcare specific industry groups will be expanded, and all stakeholder will collectively engage in the debate to solve the problems and ultimately, save lives.

Next Steps: Identify points of contacts for all of the stakeholder groups and convene a discussion forum.

The URL references for the information contained in this document are provided at the end. The Work Group acknowledges the efforts of Carla Dancy Smith in compiling this Analysis. Please contact HIMSS' staff liaison to the Medical Device Security Work Group at [lgallagher@himss.org](mailto:lgallagher@himss.org) or the Work Group chair Steve Lodin at [steven.lodin@roche.com](mailto:steven.lodin@roche.com) for any updates, questions or clarifications.

## Stakeholder Analysis

**Table 1: Selected Security-Related Legislation**

SELECTED LEGISLATION	SUMMARY
Government Performance and Results Act (GPRA)	<ul style="list-style-type: none"> <li>• Requires agencies to prepare multi-year strategic plans that describe their agency goals and action plan for achieving, including information technology related topics</li> <li>• Designed to ensure that results are tied to a budget</li> </ul>
Government Paperwork Elimination Act (GPEA)	<ul style="list-style-type: none"> <li>• Calls for Federal agencies to offer digital forms and accept electronic signatures</li> <li>• Requires agencies to give the public, businesses and other agencies the option of submitting information electronically</li> <li>• Mandates the use and acceptance of electronic signatures to bind such transactions</li> </ul>
Government Information Security Reform Act (GISRA)	<ul style="list-style-type: none"> <li>• Addresses the program management, evaluation and reporting aspect of Federal information technology security and establishes an oversight process</li> <li>• GISRA replaced by FISMA</li> </ul>
Gramm-Leach-Bliley Act	<ul style="list-style-type: none"> <li>• Requires Federal agencies and states to prepare cyber security guidance for financial institutions</li> </ul>
Sarbanes-Oxley Act	<ul style="list-style-type: none"> <li>• Requires more stringent financial reporting and auditing guidelines on public companies</li> <li>• Encourages the implementation of an internal compliance-oriented infrastructure, with adequate security controls, to reduce fraud and abuse and to facilitate the required accurate financial reporting</li> </ul>
Clinger-Cohen Act of 1996	<ul style="list-style-type: none"> <li>• Established an Information Technology Investment Management framework</li> <li>• Updated the model recently to include five stages of investment management maturity</li> </ul>
Health Insurance Portability and Accountability Act (HIPAA)*	<ul style="list-style-type: none"> <li>• Includes a Security Rule that includes procedures for protecting electronically transmitted personal patient health and medical data</li> </ul>
E-Government Act of 2002	<ul style="list-style-type: none"> <li>• Establishes enterprise architecture and other standards</li> <li>• Requires Federal agencies to complete a Privacy Impact Assessment (PIA) which requires IT or privacy professionals to assess whether appropriate privacy policies, procedures, and business practices – as well as applicable administrative, technical, and physical security controls – have been implemented.</li> </ul>
Federal Information Security Management Act of 2002 (FISMA)	<ul style="list-style-type: none"> <li>• Includes a section on information security requiring program management, evaluation, and reporting activities</li> <li>• Establishes a framework for ensuring effectiveness of Federal information security controls along with guidance regarding the development and maintenance of minimum standards</li> </ul>
Safe Medical Device Act (SMDA) of 1990	<ul style="list-style-type: none"> <li>• The final regulation details reporting requirements for healthcare providers and manufacturers when a medical device caused or contributed an event that either resulted (or <i>could</i> have resulted) in death or serious injury to a patient because of device failure, malfunction, improper or inadequate device design, manufacture, labeling, or user error.</li> </ul>

## Stakeholder Analysis

SELECTED SECURITY STANDARDS	SUMMARY
National Institute of Standards and Technology (NIST) 800 Series Publications	<ul style="list-style-type: none"> <li>• “Under the Computer Security Act of 1987 (P.L. 100-235), the Computer Security Division of the Information Technology Laboratory (ITL) develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, internetworking security, criteria and assurance, and security management and support. These publications present the results of NIST studies, investigations, and research on information technology security issues.</li> <li>• The publications are issued as Special Publications (Spec. Pubs.), NISTIRs (Internal Reports), and ITL (formerly CSL) Bulletins. Special Publications series include the Spec. Pub. 500 series (Information Technology) and the Spec. Pub. 800 series (Computer Security). Computer security-related Federal Information Processing Standards (FIPS) are also included.”</li> <li>• Under FISMA provisions will develop standards to be used by the Federal agencies to categorize information and information systems; will develop guidelines for identification of national security information and information systems and related categories and information security requirements.</li> </ul>
Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*	<ul style="list-style-type: none"> <li>• A process that applies to all services, components, activities and their contractors or agents</li> <li>• “Establishes a standard DoD-wide process, set of activities, general tasks, and a management structure to certify and accredit management Information Systems (IS) that will maintain the Information Assurance (IA) and security posture of the Defense Information Infrastructure (DII) throughout the lifecycle of the system.”</li> <li>• Policies are set out in DoD 8510.1-M; derived from DoD Directive 8500.1, Information Assurance.</li> <li>• A <i>process</i> which implements policy, assigns responsibilities and prescribes procedures for certification and accreditation of information systems, including information systems, networks, and sites in DoD.</li> <li>• The foundational document of the DITSCAP is the System Security Authorization Agreement (SSAA), which is used throughout the DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify potential solutions, and maintain operational systems security.”</li> </ul>
DoD Directives	<ul style="list-style-type: none"> <li>• There are numerous other DoD specific security related directives and regulations, including, but not limited to:               <ol style="list-style-type: none"> <li>1. DoD Directive 5000.1, defense Acquisition</li> <li>2. DoD Directive 5000.1.R, Information Security Program</li> <li>3. DoD Directive 5200.28-STD, Trusted Computer System Evaluation</li> </ol> </li> </ul>
OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation <sup>SM</sup> )	<ul style="list-style-type: none"> <li>• “A tool designed for an organization that wants to understand its information security needs</li> <li>• A risk-based strategic assessment and planning technique for security”</li> </ul>
American National Standards Institute (ANSI)	<ul style="list-style-type: none"> <li>• “A private, non-profit organization (501(c)3) that administers and coordinates the U.S. voluntary standardization and conformity assessment system.</li> <li>• The Institute's mission is to enhance both the global competitiveness of U.S. business and the U.S. quality of life by promoting and facilitating voluntary consensus standards and conformity assessment systems, and safeguarding their integrity.</li> <li>• Although ANSI itself does not develop American National Standards (ANSs), it provides all interested U.S. parties with a neutral venue to come together and work towards common agreements.”</li> <li>• Security is an ancillary issue, not the primary standard addressed by this group</li> </ul>

## Stakeholder Analysis

**Table 2: Selected Security-Related Standards**

SELECTED SECURITY STANDARDS	SUMMARY
International Organization for Standardization (ISO) 17799	<ul style="list-style-type: none"> <li>• “Detailed security standard organized into ten major sections, each covering a different topic or area:               <ol style="list-style-type: none"> <li>1. Business Continuity Planning</li> <li>2. System Access Control</li> <li>3. System Development and Maintenance</li> <li>4. Physical and Environmental Security</li> <li>5. Compliance</li> <li>6. Personnel Security</li> <li>7. Security Organization</li> <li>8. Computer &amp; Operations Management</li> <li>9. Asset Classification and Control</li> <li>10. Security Policy</li> </ol> </li> <li>• Within each section are the detailed statements that comprise the standard.”</li> </ul>
Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)*	<ul style="list-style-type: none"> <li>• A process that applies to all services, components, activities and their contractors or agents</li> <li>• “Establishes a standard DoD-wide process, set of activities, general tasks, and a management structure to certify and accredit management Information Systems (IS) that will maintain the Information Assurance (IA) and security posture of the Defense Information Infrastructure (DII) throughout the lifecycle of the system.”</li> <li>• Policies are set out in DoD 8510.1-M; derived from DoD Directive 8500.1, Information Assurance.</li> <li>• A <i>process</i> which implements policy, assigns responsibilities and prescribes procedures for certification and accreditation of information systems, including information systems, networks, and sites in DoD.</li> <li>• The foundational document of the DITSCAP is the System Security Authorization Agreement (SSAA), which is used throughout the DITSCAP to guide actions, document decisions, specify IA requirements, document certification tailoring and level of effort, identify potential solutions, and maintain operational systems security.”</li> </ul>
International Electrotechnical Commission (IEC)	<ul style="list-style-type: none"> <li>• “The leading global organization that prepares and publishes international standards for all electrical, electronic and related technologies. These serve as a basis for national standardization and as references when drafting international tenders and contracts.”</li> <li>• Security is an ancillary issue, not the primary standard addressed by this group</li> </ul>
System Security Engineering Capability and Maturity Model (SSE CMM)	<ul style="list-style-type: none"> <li>• The SSE CMM Model “describes the essential characteristics of an organization’s security engineering process that must exist to ensure good security engineering.”</li> </ul>

## Stakeholder Analysis

**Table 3: Selected Healthcare Industry Standards and Accreditation Organizations**

SELECTED HEALTHCARE SECTOR STANDARDS AND ACCREDITATIONS*	SUMMARY
The Joint Commission on Accreditation of Healthcare Organizations (JCAHO)	<ul style="list-style-type: none"> <li>Evaluates medical facility compliance based on a focused set of "requirements" that are long known as essential to the delivery of good patient care</li> </ul>
CMS Core Security Requirements (CMS CSR)	<ul style="list-style-type: none"> <li>"Detail technical requirements for business partners who use IT systems to process Medicare data. Business partners must establish and maintain responsible and appropriate controls to ensure the confidentiality, integrity, and availability of Medicare data. CMS has organized the Core Security Requirements into Categories, General Requirements, Control Techniques, and Protocols. There are ten Categories               <ol style="list-style-type: none"> <li>1. Entity-wide Security Program Planning and Management Elements</li> <li>2. Access Control</li> <li>3. System Software</li> <li>4. Segregation of Duties</li> <li>5. Service Continuity</li> <li>6. Application Software Development and Change Control</li> <li>7. Application System Authorization Controls</li> <li>8. Application System Completeness Controls</li> <li>9. Application System Accuracy Controls</li> <li>10. Networks"</li> </ol> </li> </ul>
CMS Internet Security Policy	<ul style="list-style-type: none"> <li>Issued in 1998 by then named Health Care Finance Association (HCFA), it "established the basic security requirements that must be addressed for use of the Internet to transmit HCFA Privacy Act protected and/or other sensitive HCFA information." This bulletin remains in effect until canceled or superseded.</li> </ul>
URAC Information Security	<ul style="list-style-type: none"> <li>"Offers a Security Audit service that will aid health care organizations in developing and maintaining an information security protection strategy.</li> <li>Takes a comprehensive look at how organizations are dealing with a wide range of security risks within their operations, and offer recommendations for improvement to help meet the expanding number of security-based regulatory and business requirements in the health care field."</li> </ul>
NCQA Certification and Accreditation Standards	<ul style="list-style-type: none"> <li>"An independent, 501(c)(3) non-profit organization whose mission is to improve health care quality everywhere.</li> <li>NCQA evaluates health care in three different ways: through accreditation (a rigorous on-site review of key clinical and administrative processes); through the Health Plan Employer Data and Information Set (HEDIS® -- a tool used to measure performance in key areas like immunization and mammography screening rates); and through a comprehensive member satisfaction survey. Although participation in our accreditation and certification programs is voluntary, more than half the nation's HMOs currently participate. And almost 90 percent of all health plans measure their performance using HEDIS."</li> </ul>

## Stakeholder Analysis

**Table 4: Selected Stakeholder Groups**

The stakeholder mission and description statements are broad, unless something directly related to the security in medical devices issue was available on their website.

A. Healthcare Professionals: including providers and payors;

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
Health Information Management Systems Society, (HIMSS); Privacy and Security Task Force; Security in Medical Devices Work Group	<p>The mission of the Healthcare Information and Management Systems Society (HIMSS) is to be the trusted source for knowledge, advocacy, leadership, collaboration, and community affiliation.</p> <p>Medical devices and systems represent a growing risk with respect to the privacy and security of the health information, including patient-identifiable data, they contain. Hospitals and similar healthcare organizations typically have 300% to 400% more medical equipment than medical IT devices and two trends are contributing to the significance of this security risk: Medical devices and systems are being designed and operated as special purpose computers ... more features are being automated, increasing amounts of health information, is being collected, analyzed and stored in these devices</p> <p>There has been a rapidly growing integration and interconnection of disparate medical (and information) technology devices and systems where health information is being increasingly exchanged</p> <p>The security risk associated with medical devices and systems is increasing, so there is a need for HIMSS to address this topic.</p> <p>The Medical Device Security Work Group has been formed to address the need for coordinated understanding and direction on this topic.</p>
American College of Clinical Engineering (ACCE); HIPAA Task Force	<p>Nonprofit professional organization primarily of clinical engineers, biomedical engineers and healthcare technologists that promotes the safe and effective application of technology to patient care <i>and</i> whose security related activities have included:</p> <p><u>Advocacy &amp; Education</u></p> <ul style="list-style-type: none"> <li>• Develop presentations on security &amp; medical devices</li> <li>• Developed Guidance document for Security's implications for medical technology (jointly published by ACCE/ECRI)</li> </ul> <p><u>HIPAA Task Force</u> (formed in 2001)</p> <ul style="list-style-type: none"> <li>• Address security's implications for medical devices &amp; systems (primarily focusing on Security Rule)</li> </ul>
ECRI	<p>Nonprofit research and consulting organization whose constituents include:</p> <ul style="list-style-type: none"> <li>• Government (HHS/FDA/CDRH/AHRQ) &amp; international</li> <li>• Healthcare providers (consumers &amp; operators of medical technology)</li> <li>• clinical engineers, biomedical engineers, healthcare technologists</li> <li>• Health plans</li> <li>• Manufacturers</li> </ul> <p>ECRI services include:</p> <p><u>Medical technology</u></p> <ul style="list-style-type: none"> <li>• Research, evaluations, technology assessment (i.e., publishes <i>Health Devices</i>)</li> <li>• Consultation</li> </ul> <p><u>Patient Safety</u></p> <p><u>Research &amp; Education</u></p> <p>Publications (including articles &amp; guides) and presentations on security issues associated with medical technology</p>

## Stakeholder Analysis

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
Association for the Advancement of Medical Instrumentation (AAMI)	Nonprofit organization committed to serve as <ul style="list-style-type: none"> <li>• A forum for the exchange of information on medical instrumentation and technology and</li> <li>• A resource for the industry, the professions and government for national and international standards</li> </ul>
National Quality Forum (NQF)	The National Quality Forum is a private, not-for-profit membership organization created to develop and implement a national strategy for healthcare quality measurement and reporting. <b><i>The mission of the NQF is to improve American healthcare through endorsement of consensus-based national standards for measurement and public reporting of healthcare performance data that provide meaningful information about whether care is safe, timely, beneficial, patient-centered, equitable and efficient.</i></b>
Security Health Care Certification and Accreditation Workgroup co-facilitated by URAC/NIST/WEDI	<p>Mission</p> <ul style="list-style-type: none"> <li>• Bring together key stakeholders from the public and private sectors to facilitate communication and consensus on best practices for information security in healthcare.</li> <li>• Promote the implementation of a uniform approach to security practices and assessments by developing white papers and crosswalks, and provide educational programs, as appropriate.</li> </ul> <p>Goals</p> <ul style="list-style-type: none"> <li>• Review NIST Special Publications 800-37 and 800-53 for possible use in the healthcare sector.</li> <li>• Review other security standards such as the HIPAA Security Rule, ISO 17799, CMS' CAST requirements, Systems Security Engineering Capability Maturity Model (SSECCMM), CMS Internet Security Requirements, among other possible requirements or standards.</li> <li>• Develop a common set of health care security standards that will cover security policies, procedures, controls and auditing practices.</li> </ul>

### B. Information Security Professionals

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
The Information Systems Security Association (ISSA)®	The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

### C. Consumers/Users/Patients

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
The Leapfrog Group	Composed of more than 150 public and private organizations that provide health care benefits, The Leapfrog Group works with medical experts throughout the U.S. to identify problems and propose solutions that it believes will improve hospital systems that could break down and harm patients. Representing more than 34 million health care consumers in all 50 states, Leapfrog provides important information and solutions for consumers and health care providers. The Leapfrog Group focuses on the quality of certain aspects of care relevant to urban area hospitals. Patients are usually in fragile health when in the hospital and the consequences of preventable medical mistakes can be serious.

## Stakeholder Analysis

### D. Government Regulators

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
Federal Drug Administration (FDA), Center for Devices and Radiological Health (CDRH)	FDA's Center for Devices and Radiological Health is responsible for ensuring the safety and effectiveness of medical devices and eliminating unnecessary human exposure to man-made radiation from medical, occupational and consumer products. There are thousands of types of medical devices, from heart pacemakers to contact lenses. Radiation-emitting products regulated by FDA include microwave ovens, video display terminals, and medical ultrasound and x-ray machines.
Health and Human Services (HHS)	

### E. Manufacturers

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
National Association of Manufacturers (NAM)	The NAM's mission is to enhance the competitiveness of manufacturers and to improve American living standards by shaping a legislative and regulatory environment conducive to U.S. economic growth, and to increase understanding among policymakers, the media and the public about the importance of manufacturing to America's economic strength. The NAM is the nation's largest industrial trade association. We represent 14,000 members (including 10,000 small and mid-sized companies) and 350 member associations serving manufacturers and employees in every industrial sector and all 50 states.
National Electrical Manufacturers Association (NEMA)	NEMA is a federation of over 50 diverse product sections that are grouped into eight divisions. NEMA's 450 member companies manufacture products ranging from x-ray machines and CT scanners to motors and generators, lamps, luminaires, cable tray, building wire, enclosures, traffic controls, nurse call systems, batteries, residential controls, etc. NEMA's <i>Diagnostic Imaging &amp; Therapy Systems Division</i> has produced numerous white papers & guidelines on issues related on HIPAA and medical device security

### References:

[1] Links to the selected security related legislation mentioned and/or quoted are provided:

SELECTED LEGISLATION	URLS
Government Performance and Results Act (GPRA)	<a href="http://www.whitehouse.gov/omb/mgmt-gpra/">http://www.whitehouse.gov/omb/mgmt-gpra/</a>
Government Paperwork Elimination Act (GPEA)	<a href="http://www.whitehouse.gov/omb/fedreg/gpea2.html">http://www.whitehouse.gov/omb/fedreg/gpea2.html</a>
Government Information Security Reform Act (GISRA replaced by FISMA)	<a href="http://www.whitehouse.gov/omb/memoranda/m01-08.pdf">http://www.whitehouse.gov/omb/memoranda/m01-08.pdf</a>
Gramm-Leach-Bliley Act	<a href="http://banking.senate.gov/conf/">http://banking.senate.gov/conf/</a>
Sarbanes-Oxley Act	<a href="http://banking.senate.gov/pss/acctfrm/conf_rpt.pdf">http://banking.senate.gov/pss/acctfrm/conf_rpt.pdf</a>
Clinger-Cohen Act	<a href="http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html">http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html</a>
Health Insurance Portability and Accountability Act (HIPAA)	<a href="http://www.cms.hhs.gov/hipaa/">http://www.cms.hhs.gov/hipaa/</a>

## Stakeholder Analysis

SELECTED LEGISLATION	URLS
E-Government Act of 2002	<a href="http://www.cio.gov/documents/e_gov_act_2002.pdf">http://www.cio.gov/documents/e_gov_act_2002.pdf</a>
Federal Information Security Management Act of 2002 (FISMA)	<a href="http://www.fedcirc.gov/library/legislation/FISMA.html">http://www.fedcirc.gov/library/legislation/FISMA.html</a>

[2] Links to the selected security standards mentioned and/or quoted are provided:

SELECTED SECURITY STANDARDS	URLS
National Institute of Standards and Technology (NIST) 800 Series Publications	<a href="http://csrc.nist.gov/publications/">http://csrc.nist.gov/publications/</a>
Department of Defense Information technology Security Certification and Accreditation Process (DITSCAP)	<a href="http://www.tricare.osd.mil/tmis_new/Policy/DoD/i520040p.pdf">http://www.tricare.osd.mil/tmis_new/Policy/DoD/i520040p.pdf</a>
Various DoD Directives	<a href="#">See DOD Section, Policy and Guidance</a> <a href="http://www.tricare.osd.mil/tmis_new/Policy/DoD/p52001r.pdf">http://www.tricare.osd.mil/tmis_new/Policy/DoD/p52001r.pdf</a>
OCTAVE <sup>®</sup> (Operationally Critical Threat, Asset, and Vulnerability Evaluation <sup>SM</sup> )	<a href="http://www.cert.org/octave/">http://www.cert.org/octave/</a>
American National Standards Institute (ANSI)	<a href="http://www.ansi.org/">http://www.ansi.org/</a>
International Organization for Standardization (ISO) 17799	<a href="http://www.iso17799software.com/">http://www.iso17799software.com/</a>
International Electrotechnical Commission (IEC)	<a href="http://www.iec.ch/">http://www.iec.ch/</a>
System Security Engineering Capability and Maturity Model (SSE CMM)	<a href="http://www.sse-cmm.org/">http://www.sse-cmm.org/</a>

[3] Links to the selected healthcare related standards mentioned and/or quoted are provided:

SELECTED HEALTHCARE SECTOR STANDARDS/ACCREDITATIONS	URLS
The Joint Commission on Accreditation of Healthcare Organizations (JCAHO)	<a href="http://www.jcaho.org/">http://www.jcaho.org/</a>
CMS Core Security Requirements (CMS CSR)	<a href="http://www.cms.hhs.gov/manuals/pm_trans/AB03005.pdf">http://www.cms.hhs.gov/manuals/pm_trans/AB03005.pdf</a>
CMS Internet Security Policy	<a href="http://www.cms.hhs.gov/it/security/docs/internet_policy.pdf">http://www.cms.hhs.gov/it/security/docs/internet_policy.pdf</a>
URAC Security Audit Service	<a href="http://www.itsecurity.com/tecsnews/jan2004/jan185.htm">http://www.itsecurity.com/tecsnews/jan2004/jan185.htm</a>
NCQA Certification and Accreditation Standards	<a href="http://www.ncqa.org/index.asp">http://www.ncqa.org/index.asp</a>

## Stakeholder Analysis

[4] Links to the selected stakeholder groups mentioned and/or quoted are provided:

### A. Healthcare Professionals, including providers and payors

SELECTED STAKEHOLDER GROUPS	URLS
Health Information Management Systems Society, (HIMSS); Privacy and Security Task Force; Security in Medical Devices Work Group	<a href="http://www.himss.org/ASP/index.asp">http://www.himss.org/ASP/index.asp</a>
American College of Clinical Engineering (ACCE)	<a href="http://www.accenet.org">http://www.accenet.org</a>
National Quality Forum (NQF)	<a href="http://www.qualityforum.org/">http://www.qualityforum.org/</a>
ECRI	<a href="http://www.ecri.org">http://www.ecri.org</a>
Association for the Advancement of Medical Instrumentation (AAMI)	<a href="http://www.aami.org">http://www.aami.org</a>

### B. Information Security Professionals

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
The Information Systems Security Association (ISSA)®	<a href="http://www.issa.org/aboutissa.html">http://www.issa.org/aboutissa.html</a>

### C. Consumers/Users/Patients

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
The Leapfrog Group	<a href="http://www.leapfroggroup.org/">http://www.leapfroggroup.org/</a>

### D. Government Regulators

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
Federal Drug Administration (FDA)	<a href="http://www.fda.gov/cdrh/">http://www.fda.gov/cdrh/</a>
Health and Human Services (HHS)	

### E. Manufacturers

SELECTED STAKEHOLDER GROUPS	MISSION/DESCRIPTION
National Association of Manufacturers (NAM)	<a href="http://www.nam.org/index.asp?TrackID=">http://www.nam.org/index.asp?TrackID=</a>
National Electrical Manufacturers Association (NEMA)	<a href="http://www.nema.org">http://www.nema.org</a>