230 E. Ohio Street, Suite 500
Chicago, IL 60611-3269

Tel 312 664 4467
Fax 312 664 6143

www.himss.org

January 21, 2009

The Honorable Henry Waxman Chairman Committee on Energy and Commerce U.S. House of Representatives 2125 Rayburn House Office Building Washington, DC 20510	The Honorable Joe Barton Ranking Member Committee on Energy and Commerce U.S. House of Representative 2322-A Rayburn House Office Building Washington, DC 20510

Dear Chairman Waxman and Ranking Member Barton:

On behalf of the Board of Directors and members of the Healthcare Information and Management Systems Society (HIMSS), we are writing to express our support for health information technology (IT) provisions included in the economic stimulus legislation, the American Recovery and Reinvestment Plan of 2009, released by the House Appropriations, Energy and Commerce, and Ways and Means Committee during the week of January 12, 2009. The provisions provide for the necessary investment in health IT infrastructure improvements for healthcare throughout the U.S.

HIMSS focuses exclusively on ensuring the optimal use of healthcare information technology and management systems for the betterment of healthcare. Founded in 1961, HIMSS represents more than 20,000 individual members – of which 73% work in provider settings – and over 350 corporate members that collectively represent organizations employing millions of people.

While we support the legislation, please note that we urge the Committees to appropriately address the role of current standards harmonization and health IT certification organizations, as well as reconsider privacy and security provisions, a provision concerning the role of federal government in developing and maintaining electronic health record (EHR) technology, and a provision that addresses the expansion of medical health informatics education programs. Please refer to Appendix A for a detailed listing of our feedback and recommendations concerning the privacy and security provisions.

We believe that any funding for health IT authorized and appropriated in economic stimulus legislation should include specific requirements concerning how to best allocate the funding. We applaud the Committees' inclusion in legislation to incentivize use of certified EHR technologies, the establishment of competitive grants programs, and leveraging the reimbursement structure of Medicare and Medicaid to foster the use of certified EHR technologies among providers. And, by establishing a senior leadership position for health IT (the Office of the National Coordinator for Health Information Technology), the legislation takes the necessary steps to provide for oversight and direction of some new health IT initiatives, while

ensuring the essential leadership in efforts to establish a Nationwide Health Information Network (NHIN).

As you continue to examine and develop economic stimulus legislation, we urge you to address the critical role that the Healthcare Information Technology Standards Panel (HITSP) and the Certification Commission for Healthcare Information Technology (CCHIT) play in standards harmonization and certification of health IT products. Since its inception in 2005 by ANSI (the American National Standards Institute), HITSP has led the national effort to harmonize interoperability standards to facilitate the secure exchange of health information. Utilizing the nearly century-old open, inclusive, collaborative volunteer-driven approach developed and tested by ANSI, HITSP's harmonization work incorporates the views of 565 organizational members, of which 22 are consumer organizations, to address such areas as EHRs, biosurveillance, consumer empowerment, medication management, quality, and population health.

Building on standards harmonization that is made possible through HITSP, CCHIT functions as a recognized certification body (RCB) for EHRs and their networks. To date, CCHIT has certified more than 150 EHR products, representing 50% of all vendors in the market and 75% of the overall EHR market to date. CCHIT has helped streamline the EHR market by serving as a trusted source to guide providers when adopting health IT products. CCHIT has also aided in fostering interoperability among products through implementation of its standards-based criteria.

The achievements of and the resources allocated to ensure the mission of these organizations should not be minimized. Policy should continue to recognize the important role that HITSP and CCHIT play in standards harmonization and the certification of health IT products.

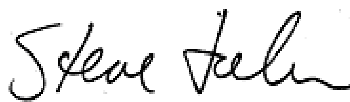
We urge you to consider removing from the legislation the requirement for "the National Coordinator for Health Information Technology to support the development, routine updating, and provision of a qualified EHR technology, unless the Secretary of Health and Human Services (HHS) determines that the needs and demands of providers are being substantially and adequately met through the marketplace." Today, EHR technology is widely available in a competitive market in which vendors compete on the basis of price, quality, and functionality of a product. As mentioned, above, over 150 EHR products have already been certified by CCHIT and are available for ambulatory and acute care providers. Just like we do not support the federal government developing products or services to compete in the private sector, we do not support the federal government developing EHR technology.

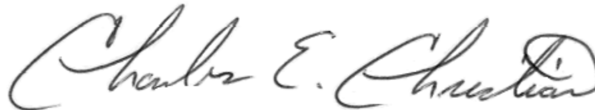
In order to ensure the rapid and effective utilization and development of health IT, we ask that the assistance provided to institutions to establish or expand medical health informatics education programs is inclusive of the needs of the nursing profession. Nurses constitute the largest single group of healthcare workers, and as such, require basic and continuing education on informatics concepts and foundational components of achieving the implementation and integration of information systems throughout the healthcare system. Establishment of new or expanded nursing informatics programs would further inform and engage these key stakeholders and support their leadership in the widespread adoption, implementation and use of EHR systems.

The health IT provisions included in legislation by the House Appropriations, Energy and Commerce, and Ways and Means Committee reflect necessary measures to develop and maintain a robust IT infrastructure for healthcare. The provisions are sure to create jobs and enable providers to implement the necessary and appropriate technologies to improve the quality and reduce the cost of healthcare.

Thank you for addressing the critical role that health IT has in transforming healthcare in the U.S. For additional information concerning how health IT can transform healthcare, please access HIMSS' detailed report *Enabling Healthcare Reform Using Information Technology*. We welcome the opportunity to discuss any of the content in this letter in further detail. We can be reached by phone at (312) 915-9225 or by email at slieber@himss.org and cchristian@gshvin.org.

Sincerely,





H. Stephen Lieber, CAE	Charles E. Christian, FCHIME, FHIMSS
HIMSS President/CEO	Chair, HIMSS Board of Directors
	Director IS/CIO
	Good Samaritan Hospital

Appendix A

HIMSS Letter of Support for Health IT Provisions in Economic Stimulus Legislation
Request for Reconsideration of Privacy and Security

Recognizing the necessity and value of access to, and exchange of, electronic health information in assuring safe, high-quality health care, HIMSS supports the inclusion of measures that enable essential and appropriate access ***without imposing undue or unreasonable requirements that are technically or operationally impractical, or otherwise could result in unintended consequences.***

Knowing that it is critical that privacy provisions be addressed in order to establish and maintain a bond of trust and to address the concerns of patients, providers and all that participate in the health system, ***HIMSS urges Congress to put in place a process that allows dialog and input from all stakeholders in order to create a workable and practical privacy/security policy framework to protect personal health information.***

Federal breach notification requirement

HIMSS supports the notification of individuals whose information may have been compromised. However,

- We do not support a requirement for a broad, public notification of a potential breach, as this increases overall security risk.
- We further believe that breach notification provisions should consider/be triggered by the risk of harm that may result from the disclosure, as opposed to merely the number of records breached. Redundant notifications or notifications where there is little possibility of further harm would only confuse and worry patients.
- We are concerned that the bill as written may result in confusion regarding notification responsibilities among Covered Entities (CEs) and Business Associates in Health Information Exchange scenarios, potentially resulting in redundant/confusing notifications to patients.

Accounting of Certain PHI Disclosures If Covered Entity Uses EHR

HIMSS supports this provision in principle, but recognizes that technology and operational practices in use today may not allow CEs to immediately meet this requirement. We therefore recommend that this provision be limited to disclosures of structured information, and that its implementation be tied to health IT product certification efforts to enable it to be implemented as supporting technology becomes available, and so as to avoid significant cost and operational disruption to the current health system.

Please note that these remarks included in Appendix A are the result of expert input from HIMSS Privacy & Security Taskforce volunteers. As of January 21, 2009, they have not yet been reviewed or approved by our Board of Directors.

We recognize that this legislation directs the Secretary of HHS to consider what types of technologies are available and feasible for improving privacy and security that can be built into technical standards and that it establishes an implementation timeline. We believe these types of approaches ultimately will create more valuable information for patients and allow health care organizations to devote more resources to the delivery of care.

We respectfully note the following complexities due to the current language in the bill:

- Identifying a "disclosure", as defined by the legislation, within treatment and healthcare operations will need new interpretations. For example, within a hospital setting a communication to a non-employee who has privileges (a contractor) is a disclosure, when the same communication to an employed doctor is not. Therefore, CEs will likely be required to spend time sorting out what is a disclosure as opposed to what is considered an internal communication.
- The definition of an electronic health record (EHR) provided in the legislation is: "an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff within a single organization." This definition is extremely broad and could be interpreted to cover a simple e-mail, faxes and/or many other independent forms of recordkeeping – patient safety, internal billing, e-prescribing, databases, etc.

Prohibition on Sale of Protected Health Information

HIMSS opposes these provisions, as currently written, as they add complexities and burdens that could undermine quality improvement, patient safety and delivery of care. HIMSS therefore recommends that the Secretary be tasked to study this issue in greater detail before enacting applicable law.

- These complexities include, but may not be limited to, the definition of "sale," purposes of the sale; definition of an "individual's health information" (e.g., de-identified vs. identifiable); property and ownership issues; and the need for a balance between public and private good and research-related concerns.
- The prohibition applies to "direct or indirect remuneration" in exchange for any information unless there is consent or authorization. This is effectively a sweeping prohibition for healthcare operations and associated functions. As an example in the area of research and public health activities, many parties provide access to databases for research at a price. The current price reflects the value of the database and not the cost of transmittal. This means the financial arrangements for many research, drug safety, surveillance and other useful activities would no longer be permissible. Also, the burden of the individual consent requirements could undercut the value of these activities.

Please note that these remarks included in Appendix A are the result of expert input from HIMSS Privacy & Security Taskforce volunteers. As of January 21, 2009, they have not yet been reviewed or approved by our Board of Directors.

- The definition of healthcare operations includes items such as:
  (a) conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines
  (b) population-based activities relating to improving health or reducing health care costs
  (c) protocol development

  However, there do not seem to be exceptions for these in the bill, even though groups may want to pool access to databases for these purposes. These may very well entail financial relationships involving direct or indirect remuneration.

Enforcement by State Attorney Generals and Local Law Enforcement Agencies

HIMSS is opposed to giving state attorneys general the ability to bring civil action as a means of enforcing the HIPAA Privacy Rule. The Department of Justice and the HHS Office for Civil Rights (OCR) already have substantial authority to pursue criminal and civil enforcement of the HIPAA Privacy Rule. Instead, we suggest that the legislation focus on enhancing the ability of OCR to conduct its enforcement activities. Further:

- We are concerned that political pressures could influence litigation at the state level while providing little or no increased guarantee of compliance with the rules by giving such authority to the states. In contrast, OCR is subject to procedural limitations on the abuse of prosecutorial powers that would not necessarily apply to state attorneys general.
- We note that state attorneys general already have sufficient authority under existing law to enforce stricter state laws regarding the misuse of personal health information and prosecute against unfair and deceptive practices. In the event they uncover information related to suspected HIPAA violations, they may refer that information to the OCR and create state liaisons to ensure that office uses the information in a timely and effective manner.

Please note that these remarks included in Appendix A are the result of expert input from HIMSS Privacy & Security Taskforce volunteers. As of January 21, 2009, they have not yet been reviewed or approved by our Board of Directors.