April 16, 2014

The Honorable Fred Upton
Chairman, Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Upton:

In response to your request for feedback on the *Sensible Oversight for Technology Which Advances Regulatory Efficiency (SOFTWARE) Act of 2013*, the undersigned organizations are pleased to submit our comments on an oversight framework for health information technology (IT) that improves patient safety, promotes innovation, and reduces regulatory duplication.

The contents of this letter are drawn from the work of the Bipartisan Policy Center (BPC), Health IT Now, and HIMSS—namely BPC's report, *An Oversight Framework for Assuring Patient Safety in Health Information Technology*; Health IT Now's letter to the FDASIA Work Group dated July 16, 2013 and its testimony to the Energy and Commerce Committee on March 20, 2013 and November 19, 2013; and HIMSS' letter to the Department of Health and Human Services (HHS) Secretary dated November 6, 2013—along with a series of stakeholder meetings convened by BPC, Health IT Now, and HIMSS.

We believe Congress should update the statutory framework to provide clarity that clinical and administrative software should not be regulated as a medical device, a definition which Congress enacted more than forty years ago.

We support a flexible, risk-based oversight framework for clinical software to promote patient safety. To be effective, such a framework should:

- Recognize the important role that health IT plays in improving the quality, safety, and cost-effectiveness of care;
- Assure that patient safety is a shared responsibility that involves the entire health care system;
- Balance both costs and benefits;
- Ensure clear, consistent, and non-duplicative language and oversight;
- Be affordable to those expected to bear direct and indirect compliance costs; and
- Avoid adding burdens that inhibit or delay improvements to systems that improve care delivery and safety.

We appreciate HHS' recognition, as outlined in the *FDASIA Health IT Report: Proposed Strategies and Recommendations for a Risk-Based Framework* released on April 3, 2014, that clinical and administrative software (described as health management and administrative functionalities in the report) should not be regulated as a medical device.

There are three important issues Congress should consider:

1. Clearly define product attributes that would be subject to FDA regulation as a device;
2. Establish a framework for adopting or revising regulatory and oversight pathways needed to accommodate the changing marketplace; and
3. Assure the extension of legal protections that will encourage patient safety reporting by health IT developers and vendors, which can be accomplished through further clarity by HHS of existing law.

Addressing these three concepts will promote clarity in the market to significantly advance new technologies that will improve health outcomes and lower health costs. Our comments—summarized in the form of principles associated with establishment of definitions, standards, and reporting—are outlined in detail below.

Establishment of Definitions

The legislative proposal that has been introduced in the House seeks to clarify the types of technologies that would fall within the FDA's jurisdiction. Generally, the bill seeks to define technologies within three categories: medical software; clinical software; and health software.

We believe any framework for patient safety in health IT should be risk-based, flexible, and promote innovation. The scale and scope of any oversight requirements intended to ensure patient safety in health IT should be correlated to the potential risk of harm to patients. Existing FDA medical device regulations are oriented toward devices that change infrequently, where the primary patient risk is associated with the design and manufacturing which is seldom customized based on the needs of the user. This framework does not align well with the current and anticipated nature of health IT.

We believe an effective risk-based framework will accommodate the full range of health IT software, and will include alternatives to FDA medical device regulation for much of health IT software. Risk should be assessed principally by a technology's potential to harm a patient as well as the degree to which a health care professional has a reasonable opportunity to intervene.

It is within this context that we offer comments on the definitions of the various technologies to assist the Committee in further refining its legislation.

1. **Medical Devices.** FDA appropriately has authority to regulate traditional medical devices including but not limited to:

    - Diagnostic devices that initially capture physical, chemical, biologic, and similar information directly from humans or animals (x-ray machines, glucose meters, etc.)
    - Medical devices with physical parts that are used by patients (wheel chairs, prosthetics, etc.)
    - Devices with physical parts and attributes used by physicians for treatments or therapies (surgical devices, infusion pumps, etc.)

    Software that is integral to the functioning of such devices should be under FDA regulatory authority. In addition, stand-alone software that presents a high risk of potential patient harm, with limited opportunity for intervention from a learned intermediary may require additional scrutiny for regulation by the FDA. Where software or related technology is appropriately regulated by the FDA as a medical device, we do not believe there should be any change to FDA authority.

    We believe it is important to recognize that FDA should be encouraged to continue to exercise enforcement discretion within the category of medical device software, based on assessments of risk as well as the costs and benefits of regulation.

2. **Clinical Software.** Clinical software, or software and health IT that forms the basis for health information systems, health information exchange, clinical workflow, electronic health records, most clinical decision support, and subsequent transmission, storage, or management of traditional device data or other data, should not be subject to FDA regulation as a medical device. Clinical software:

    - Is intended to be used to supplement care provided and decisions made by physicians and other health professionals.
    - Is not the sole means for capturing or acquiring data from a medical device being used to aid in the direct diagnosis, diagnostic analysis, or treatment of a patient, nor does it supplant treatment decisions made by a health care professional.

    We believe that clinical software should be subject to a new risk-based oversight framework that takes into account factors such as risk relative to intended use, the cost/benefit of any proposed oversight, and the principle of shared responsibility, with the intent of ensuring patient safety and appropriate improvements in quality, effectiveness, and efficiency of care delivery.

Additionally, it is important that this new oversight framework act in concert with and not conflict with or duplicate the medical device regulation framework. We recognize that health IT and medical devices are interwoven into a single, broad patient care ecosystem, and believe that the new health IT oversight framework can complement the existing medical device regulatory process.

3. **Health Software.**

   - Is software that captures, analyzes, changes or presents patient or population clinical data or information or administrative data, such as scheduling or claims information, and that supports administrative, financial or operational aspects of health care.
   - Is not used in the direct delivery of clinical care.
   - Acts as a platform for secondary software or as a mechanism for connectivity or to store data.

   Health software should not be regulated by the FDA or alternative oversight structures because it poses the lowest risk of potential harm.

4. **Data.** We believe data should not be treated as a medical device. The subsequent transmission and storage of patient generated data, clinician generated data, or data from a medical device should not be subject to the same controls as the device itself regardless of the category of health IT associated with the data as defined by Congress and/or by regulatory and oversight bodies (medical, clinical or administrative). We suggest explicitly recognizing this principle in any legislation.

Gaining Agreement on and Assuring the Adoption of Standards

An effective oversight framework for clinical software should include agreement on and adoption of process standards and best practices that promote patient safety in the development, implementation, and use of health IT.

A health IT oversight framework should recognize that health IT is part of a complex patient care ecosystem involving providers, product developers, vendors, a wide array of use cases, and consumers as both patients and caregivers. A systemic and flexible approach is needed that reflects shared responsibility and the complexity and evolving nature of health IT.

Gaining Agreement on Standards

1. A single national approach for identifying and gaining agreement on a broad and flexible set of standards that can be applied to a diverse range of processes, products, and settings is necessary. Such an approach should reflect good governance practices and promote public participation.

2. The bodies that participate in the implementation of this national standards consensus process should demonstrate the attributes of a "voluntary consensus body".

    - Voluntary consensus bodies are defined by OMB Circular A-119 as those that exhibit the attributes of openness, balance of interest, due process, and appeals process, and consensus.

    - Under the National Technology Transfer and Advancement Act of 1995 and OMB Circular A-119, the federal government is required to use standards developed by voluntary consensus bodies in its regulatory and procurement activities, unless the use of such standards would be inconsistent with applicable law or otherwise impractical.

3. The national approach should engage both public and private stakeholders, including but not limited to experts in patient safety, health IT, health informatics and information management, as well as clinicians, clinics, consumers, employers, health plans, hospitals and health systems, laboratories, medical device manufacturers, mobile technology companies, patient safety organizations, pharmacies, health IT companies, and the many federal and state agencies that play a role in patient safety and/or the development, implementation, or use of IT in health care.

4. To the extent possible, existing process standards should be leveraged, using international standards where applicable. Well-established standards that support patient safety in health IT already exist. Examples include those focused on quality management systems, risk management, safety, and software engineering developed by standards organizations such as the International Organizations for Standardization (ISO).

5. The federal government should adopt the standards identified and agreed upon through this national approach and assure alignment of recognized standards across federal agencies to avoid areas of conflict or duplication (e.g. those required under medical device regulation or ONC EHR certification).

Promoting Adoption of Standards

1. Those who develop, implement, and use clinical software should voluntarily adhere to federally recognized standards identified and agreed upon through the national approach described above.

2. Adherence to such standards should be demonstrated through existing or new conformity tools, which can included but not be limited to accreditation, certification, and attestation facilitated by bodies recognized by the federal government.

3. Methods to demonstrate adherence must be flexible, reflect the continued evolution and complexity of health IT and continued research and a changing evidence base. They should not be unduly burdensome or prescriptive.

4. The federal government should rely upon such conformity tools for its own regulatory processes related to clinical software and should avoid duplicative and/or conflicting regulatory requirements.

Reporting, Surveillance, and Building a Learning Health System

An effective oversight framework for clinical software should be data driven. It should support and promote reporting, sharing, and analysis of patient safety events in a non-punitive environment that maintains confidentiality and enables learning and improvement.

Assuring patient safety in health IT is a shared responsibility among the many stakeholders within the health care ecosystem. As noted in the recent Institute of Medicine (IOM) report, *Health IT and Patient Safety: Building Safer Systems for Better Care,* safety is part of a larger socio-technical system that takes into account not just the software, but also how it is used. This larger system includes technology, people, processes, organizations, and the external environment.

Reporting of patient safety events by users, developers, implementers, and patients (often referred to as "surveillance") is essential to both gaining an understanding of the nature and magnitude of health IT–related safety events and developing and implementing strategies to address risks. Aggregation and analysis of events and timely feedback to developers, implementers, and users are also crucial, so that necessary changes can quickly be made to address identified issues and to mitigate future risk.

1. **Leveraging Existing Authorities.** Rather than creating new, duplicative authorities, technical structures and approaches, existing authorities and related reporting investments, processes, and systems bodies should be leveraged, such as the *Patient Safety and Quality Improvement Act of 2005*.

2. **Integrated Reporting Structures.** Reporting structures should reflect the fact that health IT safety is part of a larger socio-technical system, with shared responsibility among developers, implementers, and users across the entire health IT life cycle. Siloed reporting systems focused solely on health IT would result in duplicative reporting, unnecessary burden, and failure to capture many events.

3. **Requirements for Reporting.** When there are legal protections as described in no. 4, developers, implementers, and users should participate in the reporting of health IT safety events, with requirements for reporting that cause death or serious harm. Such requirements already exist for many providers. This reporting can be accomplished through patient safety organizations, conformity assessment bodies, or other entities. Such reporting policies are not intended to limit or take the place of current provider reporting of patient safety issues directly to health IT vendors.

4. **Non-Punitive Environment That Encourages Reporting, Learning, and Improvement**. Creating a non-punitive environment will encourage reporting of all events, including hazards, unsafe conditions, and near misses, to support learning and improvement. As noted in the recent IOM report on patient safety and health IT, in other countries and industries, reporting systems differ with respect to their design, but the majority employs reporting that is voluntary, confidential and non-punitive. To encourage reporting and create a learning environment, HHS should extend confidentiality protections currently provided to providers, to health IT developers and vendors to expand their participation in reporting and other patient safety-related activities.

5. **Aggregation, Analysis, and Dissemination to Support a Learning Health Care System.** A system-wide approach, including the aggregation and analysis of reports which protect the confidentiality of patients, providers, products, and vendors across large populations enables identification of underlying patterns and trends, as well as emerging risks. This also supports the development and implementation of interventions to mitigate risk and enables system-wide learning and improvement. The use of common formats and standards play a key role in effective analysis of aggregated data.

6. **Efficient and Non-Duplicative Processes.** Reporting efforts should take into account existing work flows, and the burden of reporting should be minimized. Federal agency policies associated with reporting should be clear, consistent, and non-duplicative both in language and enforcement. The federal government should recognize and leverage existing reporting processes, including those that reside in the private sector, to identify health IT-

related events that cause death or serious harm with appropriate protections of privacy and confidentiality and avoid the creation of duplicative or conflicting reporting processes or systems.

Conclusion

We appreciate the opportunity to share our thoughts with you on these issues.

We look forward to working with you to ensure we promote safety and innovation as Congress moves forward in updating the laws related to health information technology regulation.

Sincerely,

Academy of Managed Care Pharmacy

Alliance for Quality Improvement and Patient Safety (AQIPS)

American Academy of Family Physicians

American College of Physician Executives (ACPE)

American Health Information Management Association (AHIMA)

American Medical Group Association (AMGA)

American Medical Informatics Association (AMIA)

American Nurses Association

American Osteopathic Association

American Society of Consultant Pharmacists

athenahealth

Bipartisan Policy Center

Cerner Corporation

College of Healthcare Information Management Executives (CHIME)

Greenway Medical Technologies

Health Fidelity

Health IT Now

HIMSS

IBM Corporation

McKesson Corporation

Newborn Coalition

Pharmacy HIT Collaborative

Software and Information Industry Association

Stanley Healthcare, a Stanley Black and Decker, Inc. Company

VTC Enterprise

WellPoint