December 13, 2013

Mr. Adam Sedgewick
Senior Information Technology Policy Advisor
National Institute of Standards and Technology
Information Technology Laboratory
Gaithersburg, MD 20899
Submitted electronically to: csfcomments@nist.gov

Re: Request for Comments on the Preliminary Cybersecurity Framework

Dear Mr. Sedgewick:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to submit comments regarding this Request for Comment (RFC) on the Preliminary Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) in the October 29, 2013, issue of the *Federal Register*.

CHIME is an executive organization dedicated to serving chief information officers (CIOs) and other senior healthcare IT leaders. With more than 1,400 CIO members and over 100 healthcare IT vendors and professional services firms, CHIME seeks to shape the future of healthcare through IT leadership. Healthcare IT professionals share the vision of a safe and secure national critical infrastructure and support a consistent, iterative approach to identifying, assessing and managing cybersecurity risk.

CHIME believes the approach articulated by NIST to "encourage organizations to consider cybersecurity risk as a priority similar to financial, safety and operational risk," is the correct one. And we support the tenet of a standardized method to assess and manage cybersecurity risk, which can be broadly applied to public sector, private sector and critical infrastructure operators of all sizes.

As NIST and subsequent stewards of the Framework consider its use among critical infrastructure owners and operators, we wish to identify some of the unique distinctions of the healthcare sector's data security environment, such as:

- **REGULATIONS:** Healthcare is a highly-regulated industry, with sometimes divergent guidance on data security and privacy as applied by various federal entities, state regulators and business agreements;
- **SETTINGS:** The ability of individual physicians to implement the framework in an ambulatory setting differs greatly from the ability of large inpatient facilities;

- **RESOURCES:** Small, rural, and Critical Access Hospitals have unique resource limitations when implementing complex programs, especially those that involve new technology;
- **FINANCIAL MODELS:** Financial incentives for the kinds of investment needed to bring healthcare into compliance are nonexistent through current policy – despite disincentives (penalties) for failing to digitize patient information;
- **DATA EXCHANGE:** Healthcare providers are only recently beginning to exchange data beyond their four walls and it is important that policies support such health information exchange (HIE) activities;
- **MOBILE HEALTH:** Mobile device use within healthcare delivery is growing rapidly and various applications are evolving quickly.

In response to these identified characteristics, we offer the following high-level recommendations.

Use Compatible Versions & Coordinate Regulatory Applications
All federal agencies engaged in the regulation of healthcare should use a compatible instantiation of this Framework for risk identification, assessment and management. Specifically, we want to ensure a coordinated approach is promulgated across all agencies that regulate healthcare. Regulations meant to address gaps in cybersecurity should rely on the tenets of the Framework:

- To use existing standards, guidance, and best practices to achieve outcomes that can effectively manage cybersecurity risk and
- To use those practices developed, managed, and updated by industry to evolve with technological advances and business requirements.

Avoid Cost & Administrative Burden
Federal regulatory bodies should not use the Cybersecurity Framework to impose more cost and administrative burden on providers. Instead, the Framework should be used as an overlay to existing requirements, with an onus on the regulator to explain how those existing requirements fit into the Framework, before being incorporated into new requirements.

- **Seek a balance between flexibility and prescriptive guidance:** By incorporating the Framework into new requirements regulators should seek a balance between flexibility and prescriptive guidance. HIPAA's "addressable" construct has proven to be an inefficient, ineffective mechanism to protect patient data. To determine which actions will help the healthcare sector manage cybersecurity risk, specificity is needed. So too are a specific set of standards and references.
- **Identify ways to help support under-resourced providers:** Further, regulators should identify ways to help support under-resourced providers meet new requirements. Incentives through Medicare and Medicaid reimbursement; grants for implementation and training costs should be provided to healthcare professionals expected to meet new cybersecurity requirements. And reporting / audit burdens should be minimized.

Include a Risk Counterfactual
Future iterations of the Framework should consider the inclusion of a risk counterfactual, or a way to determine what the risk of inaction is likely to be. Such an assessment tool would enable federal

College of Healthcare Information Management Executives, Public Policy Office
4300 Wilson Blvd., Suite 250 · Arlington, VA 22203
Phone: (734) 665-0000 · Fax: (734) 665-4922 · staff@cio-chime.org · www.cio-chime.org

agency and private sector operators to communicate, in business terms, the risk of not implementing / funding / staffing specific security and privacy initiatives.

Develop a Toolkit Suite for Implementation
The preliminary Framework indicated that additional education materials and documentation is promised as deliverables with the final version of the Framework. We support this and would encourage federal officials to develop a toolkit application that would assist organizations to better understand implementation of the framework into their environments.

We hope this feedback is helpful. CHIME would like to be a resource to NIST and to subsequent efforts to update / improve the Framework by helping lawmakers understand the challenges and opportunities of implementing cybersecurity protocols in healthcare.

If there are any questions about our comments or more information is needed, please contact Sharon Canner, Sr. Director of Public Policy, at scanner@cio-chime.org or (703) 562-8834. CHIME looks forward to a continuing dialogue with your offices on this and other important matters.

Sincerely,

Russell P. Branzell
President & CEO
CHIME

George T. Hickman
CHIME Board Chair
Executive VP & CIO
Albany Medical Center

College of Healthcare Information Management Executives, Public Policy Office
4300 Wilson Blvd., Suite 250 · Arlington, VA 22203
Phone: (734) 665-0000 · Fax: (734) 665-4922 · staff@cio-chime.org · www.cio-chime.org