March 11, 2022

Dawn O'Connell
Assistant Secretary for Preparedness and Response
Office of the Assistant Secretary for Preparedness and Response
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Ms. O'Connell,

On behalf of our nearly 30 member companies of the HIMSS Electronic Health Record Association (EHRA), we appreciate the opportunity to offer comment regarding national health security threats, challenges, and promising practices. EHRA member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using electronic health records (EHRs) and other health IT across the United States. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable health information technology. Throughout the COVID-19 pandemic, provider-based health IT, including EHRs, has been a prime source of data critical for providers and public health officials. Additionally, EHRs and health information networks play an important role when natural disasters strike where connectivity enables access to one's record when displaced.

From these events, we have learned that waiting for an emergency to arise to address data needs is too late. Proactive emergency preparedness is critical to minimize delays in response to crises, and enable rapid coordination between health IT developers, their healthcare provider clients, and their federal, state, and local partners. Proactive preparedness and coordination can enable the rapid sharing of critical data already routinely collected in EHRs and other health IT systems to allow policymakers to be nimble and data-driven in their response plans.

To foster improved disaster preparedness of critical infrastructure providers, the federal government should go beyond prioritizing investment in physical and technical architecture to focus on building relationships with industry. Physical and technical infrastructure might include building on national networks to enable rapid standards-based data access and exchange between the government and private sector, while relationship building will improve trust and coordination for everything from national disasters to cyber incidents.

We therefore strongly urge that ASPR and other HHS agencies work closely with federal and state agencies, including ONC and CDC, as well as industry organizations such as the EHRA, the American Immunization Registry Association (AIRA), the Association of State and Territorial Health Officials (ASTHO), the Council of State and Territorial Epidemiologists (CSTE), and Healthcare and Public Health Sector Coordinating Council (HSCC) to maintain communication and collaboration challenges to facilitate improved preparedness and the ability to respond more quickly and with greater focus.

As the pandemic unfolded, our members were challenged to address the many reporting and data sharing requirements that our clients faced. Many of these requests required changes to health IT that only our members could provide to their clients. Not until we reached out and established communications to the various agencies and organizations involved were we able to respond more quickly and focused. This collaboration also allowed to provide input into health IT/EHR capabilities that could guide upcoming approaches and alternatives that jurisdictions are considering. Our goal is to maintain these relationships moving forward to not only react, but be prepared by continually preparing for large-scale emergencies.

In that context, we offer the following feedback to the questions raised in the Request for Information.

What are the most critical national health security threats and public health and medical preparedness, response, and recovery challenges that warrant increased attention over the next five years?

EHRA Response: Pandemics, natural disasters, and cyberattacks are the top three threats that could require significant mobilization within the health care delivery system to facilitate a rapid response.

> **Pandemics** – There is a critical need to create clear reporting structures and standards that can support the needs of public health policymakers at the local, state, and federal level. The federal government should define minimum reporting standards and methodologies that states and localities can build upon to facilitate their unique needs. Reporting standards will also need to be sufficiently extensible to accommodate the unique data collection needs that will be presented by each novel disease. An extensible set of minimum standards, as well as clear channels for reporting the data via interoperability networks, will reduce the pressure on expanding data sharing and access in response to an emergency.

> **Natural Disasters** – Natural disasters can result in the destruction of local health care delivery capabilities as well as the displacement of patients. Without the robust adoption of interoperability tools and patient portals, providing clinical care for displaced people presents challenges. The lack of access to medical records reduces the ability to provide effective care both in response to the disaster and for ongoing care.

> **Cyberattacks** – The increase in electronically maintained health data and connectivity across health IT systems used by disparate organizations has raised the risk profile of healthcare providers and health IT developers. Collaboration is needed to quickly mobilize responses to cyberattacks to stop the threat from spreading and to facilitate rapid system recovery to avoid interruptions to care.

The most critical challenge in addressing these threats from a health IT perspective is structured, cross-organizational and cross-stakeholder preparedness. Depending on the threat this can take different forms.

Pandemics – Strengthening the clinical and operational data reporting during non-emergency times will exercise the capabilities required to rapidly scale reporting of additional data of either type as a new outbreak emerges. Although public health stakeholders can often leverage existing, large shared data pools in the early stages of an event, sustaining a response will require near real-time data tailored specifically to the circumstances of the emergency.

Natural disasters – Hardened infrastructure, well-defined backup procedures, and disaster recovery plans for the IT systems of healthcare facilities will bolster healthcare providers' readiness to support a response to a national disaster. Particular attention and support should be provided to small or under-resourced provider organizations. Their ability to prepare for and play a role in disaster response exercises will strengthen relationships across stakeholders and minimize the impact of a disaster on access to critical health information when treating impacted patients.

Cyberattacks – Promoting awareness and good cyber hygiene for organizations of all sizes will make significant progress toward the prevention of cybersecurity incidents. Law enforcement and other incident response teams should build relationships with stakeholders at critical infrastructure organizations, which are susceptible targets of cyberattacks, to foster trust and cooperation in the investigation and recovery processes.

What medium-term and long-term (i.e., over the next five years) actions should be taken to mitigate these challenges at the federal government and/or state, local, tribal, and territorial level?

EHRA Response:

Pandemics – CDC and ONC should continue to focus on standardizing reporting infrastructure and requirements across public health stakeholders to simplify reporting processes for provider organizations. While significant progress has been made for the needs of the COVID-19 pandemic, agencies should generalize those lessons learned to a general pandemic preparedness and response strategy.

Natural Disasters – Connectivity to data exchange frameworks can supplement disaster recovery plans for individual organizations as increased exchange with community healthcare provider partners can create natural redundancy in data availability wherever the patient may be. Governmental agencies can continue to incentivize participation in regional and national networks and evaluate how to best promote the connectivity of public health agencies and others to those networks.

Cyberattacks – Outreach and education on practical approaches, systems, and tools for all provider organizations, but particularly smaller organizations with limited resources, will be the most effective actions over the next five years.

What public health and medical preparedness, response, and recovery opportunities or promising practices should be capitalized on over the next five years?

EHRA Response: The continued advancement and expansion of national networks for data sharing and the data modernization efforts for public health will greatly support the preparedness of providers for future pandemics and natural disasters. We encourage public health agencies to investigate how they can leverage or join those networks to expand their connectivity.

Continued iteration and improved awareness about the availability of cybersecurity evaluation frameworks for healthcare organizations to evaluate and strengthen their cyber hygiene will help organizations across the healthcare delivery ecosystem improve their practices.

Sincerely,

Hans J. Buitendijk
Chair, EHR Association
Cerner Corporation

David J. Bucciferro
Vice Chair, EHR Association
Foothold Technology
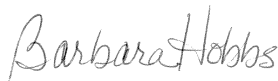
HIMSS EHR Association Executive Committee
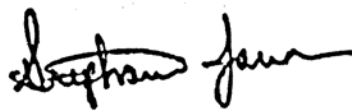
Pamela Chapman
Experity

William J. Hayes, M.D., M.B.A.
CPSI

Barbara Hobbs
MEDITECH, Inc.

Cherie Holmes-Henry
NextGen Healthcare

Stephanie Jamison
Greenway Health

Alya Sulaiman, JD
Epic