EHRA
HIMSS ELECTRONIC HEALTH RECORD ASSOCIATION

350 North Orleans Street, Suite S10000
Chicago, IL 60654

@EHRAssociation | ehra.org

November 11, 2022

Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security
245 Murray Lane Washington, D.C

Dear Director Easterly,

On behalf of the 30 member companies of the EHR Association, we are pleased to provide feedback to the Cybersecurity and Infrastructure Security Agency (CISA) regarding its implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (*Docket ID: CISA-2022-0010*). While CIRCIA covers cyber incidents impacting a broad range of sensitive data and systems, the purview of the EHR Association focuses our response primarily on aspects specifically pertaining to protected health information (PHI), for which the HIPAA Privacy Rule provides federal protections.

The HIMSS Electronic Health Record (EHR) Association is a national trade association of electronic health record (EHR) developers serving the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States, including by supporting the numerous practices they have adopted to secure sensitive patient information. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable, and secure health information technology.

We appreciate the potential for more effective collaboration on cybersecurity between industry and government and welcome the opportunity for further discussions. The Association's leadership can be reached by contacting Kasey Nicholoff at knicholoff@ehra.org.

We offer the following considerations regarding the request for information.

Sincerely,

Hans J. Buitendijk
Chair, EHR Association
Cerner Corporation

David J. Bucciferro
Vice Chair, EHR Association
Foothold Technology

AdvancedMD
Allscripts
Altera Digital Health
Athenahealth
BestNotes
CPSI

CureMD
eClinicalWorks
eMDs – CompuGroup Medical
Endosoft
Epic
Experity

Flatiron Health
Foothold Technology
Greenway Health
Harris Healthcare Group
MatrixCare
MEDHOST

MEDITECH, Inc.
Medsphere
Modernizing Medicine
Netsmart
Nextech
NextGen Healthcare

Office Practicum
Oracle Cerner
Sevocity
STI Computer Services
TenEleven Group
Varian – A Siemens Healthineers Company

HIMSS EHR Association Executive Committee

Pamela Chapman
Experity

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

Barbara Hobbs

Barbara Hobbs
MEDITECH, Inc.

Cherie Holmes-Henry
NextGen Healthcare

Stephanie Jamison
Greenway Health

Sasha TerMaat

Sasha TerMaat
Epic

Established in 2004, the Electronic Health Record (EHR) Association is comprised of 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

Criteria for "Covered Cyber Incident"

In the healthcare sector, the EHR Association recommends that CISA base the determination of whether an incident is a "Covered Cyber Incident" for the purposes of reporting under CIRCIA on (1) the degree to which the incident resulted in the risk of harm (e.g., through disruptions to operations that directly impacted patient care), (2) the scope of records compromised by the breach, and (3) whether the Covered Entity reasonably believes the incident resulted from a deliberate malicious act to gain unauthorized system access. We believe that establishing criteria that consider the practical impact of an incident for the purposes of CIRCIA reporting will strike an effective balance between minimizing the administrative burden on victims and providing potentially actionable information about credible emerging threats in the sector.

CISA should also investigate whether and how it can harmonize its reporting requirements with similar HIPAA requirements to report breaches. Criteria that describe whether a breach is reportable under HIPAA could help establish appropriate parameters for determining whether an incident compromised enough records to be reportable under CIRCIA. Mapping criteria and expected timelines for evaluating whether an incident is reportable under CIRCIA to the existing criteria for HIPAA breach reporting requirements would provide helpful guidance to Covered Entities using concepts they already understand–especially if multiple reporting obligations can be met through the submission of a single report. It would also help clarify when HIPAA breaches would not be reportable under CIRCIA, for example, if an employee inadvertently stores or transmits an individual's record in an insecure manner.

Reporting Mechanisms

The ideal format and manner in which covered entities should submit reports on covered cyber incidents will depend, in large part, on CISA's objectives for utilizing this information. Mechanisms for reporting could be as simple as a one-time contact via web form to be completed when an incident occurs, or a portal could host registered accounts for critical infrastructure providers as a means of establishing and building ongoing relationships with key contacts at these organizations.

If CISA intends that other organizations should have access to insights from reported incidents, the mechanism for gathering reports will have a downstream impact on the consumption of reports. The EHR Association suggests there is value in creating a web portal as a hub for covered entities to share threat information and report to or coordinate with federal agencies when incidents occur. There is an opportunity to create a community of threat-sharing forums, for example, in which automated feeds can be integrated into security information and event management (SIEM) systems to update indicators of compromise (IOC) and tactics, techniques, and procedures (TTP).

CISA's intended purpose of reporting will also impact the ideal balance of expectations in reporting speed and granularity. There will be a need for organizations to prioritize restoring service and mitigating the impact on their operations following a cyberattack. To that end, we recommend that CISA create a simple, internet-based web form to collect initial reporting information that does not require technical authentication or login credentials. Adding authentication requirements for entities to report incidents will delay Covered Entities' ability to submit reports during an incident since they may not be able to easily locate the individual or system that possesses the organization's login credentials to an account-based portal. CISA could still encourage Covered Entities to maintain accounts that would enable them to subscribe to threat-sharing information, however.

Content of Reports

The EHR Association recommends that CISA provide flexibility for Covered Entities to only include information they have been able to verify in the initial 72-hour report. Requiring all of the elements identified in CIRCIA at 72 hours will not be feasible and would contribute to delays in reporting and divert resources from efforts of the Covered Entity to recover and resume normal operations. Within 72 hours of noting that a Covered Cybersecurity Incident occurred, a victim organization may not have sufficient information about the full scope and impact of the breach to complete a report that includes all the elements identified in the statute. After the initial report, CISA could work with the Covered Entity to determine an appropriate point after the entity has completed recovery efforts to submit a supplemental report with details that were not available when the initial report was submitted.

The EHR Association urges CISA to consider and align with other regulatory agencies in order to avoid duplicative or contradictory reporting requirements. It will be important to harmonize reporting frameworks between the Office of Civil Rights (OCR) HIPAA breach reporting and this new CIRCIA process. To reduce unnecessary burden, clear guidance should be provided to HIPAA-regulated entities regarding the types of HIPAA breaches that should be reported to CISA and in what manner. Finally, CIRCIA should clarify that confidential information not pertinent to understanding the nature of an incident should not be submitted as part of a report. For example, in the case of a breach impacting patient records, information identifying the individual records that were impacted should not be reported. Instead, CISA should only require a broad description of the type of confidential information that was compromised.

Protections for Victim Organizations

Given the substantial legal, operational, and reputational impacts that cybersecurity incidents can have on an organization, it is essential for CISA to preserve the confidentiality of victims that submit reports. Failing to protect the confidentiality of the reports could result in a reluctance to comply with reporting expectations.

CISA should provide detailed information about its processes for protecting the confidentiality of reports and the situations in which the agency may disclose the information contained in reports to federal agencies or other entities. Disclosures to law enforcement for incident response coordination should only occur with the express consent of the reporting entity.

When using reports for threat information-sharing purposes, identifying information should be removed and advisories should focus on helping other entities make a determination of whether their systems may be impacted. Reports should be used exclusively for sharing threat information and assisting recovery efforts and should not be used for criminal or civil litigation.

Cultivating a culture of proactive reporting and information sharing – tenets central to Congress' intent when it created CIRCIA – requires that organizations victimized by cyberattacks do not feel that they will suffer additional harm by reporting.