Massachusetts Health Data Consortium

# CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements NPRM (CISA-2022-0010) Comment

This document was submitted by the Massachusetts Health Data Consortium (MHDC) and its Data Governance Collaborative (DGC) on June 3, 2024 in response to the CISA Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements NPRM (CISA-2022-0010) posted in the Federal Register on April 4, 2024 and found here:

https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

## About MHDC

Founded in 1978, MHDC, a not-for-profit corporation, convenes the Massachusetts's health information community in advancing multi-stakeholder health data collaborations. MHDC's members include payers, providers, industry associations, state and federal agencies, technology and services companies, and consumers. The Consortium is the oldest organization of its kind in the country.

MHDC provides a variety of services to its members including educational and networking opportunities, analytics services on both the administrative and clinical side (Spotlight), and data governance and standardization efforts for both clinical and administrative data (the Data Governance Collaborative/DGC and the New England Healthcare Exchange Network, respectively).

## About DGC

The DGC is a collaboration between payer and provider organizations convened to discuss, design, and implement data sharing and interoperability among payers, providers, patients/members, and other interested parties who need health data. It is a one stop interoperability resource. The DGC primarily focuses on three areas:

1. Collaboration: Development of common understanding of and specifications for data standards, exchange mechanisms, and what it means to participate in the modern health IT ecosystem
2. Education: helping members understand their regulatory obligations, the data and exchange standards they're expected to use, and modern technology and related processes
3. Innovation: Identification and development of projects and services needed to make modern health data practices and exchange a reality

## General Comments

This section comments on the general approach taken by CISA or provides comments on items that cross multiple sections of or items in the plan.

### Change Healthcare Incident and Reporting of Single Incidents Impacting Multiple Covered Entities

We recognize that this proposed rule was likely written prior to the major cyber incident at Change Healthcare this spring and urge CISA to consider how this rule would have impacted the healthcare industry at a time when it was already burdened by the outage had it been in place when the incident occurred.

This incident affects nearly every organization working in the healthcare space in some way. Most providers lost some or all of their ability to file claims, many lost their ability to request prior authorizations, and some to discover the coverage limitations of patients being seen and thus maximize their chances of reimbursement, and so on. Other types of organizations were affected in other ways.

By the rules set forth in this proposed rule, each of those organizations would be required to independently report the incident not of their making and located within a third party because it significantly disrupted their business practices. CISA would likely have gotten hundreds of thousands of reports, if not millions (with supplemental reporting considered) about a single incident. Providers would have been asked to calculate the costs on their business at a time when their business was under extreme stress and likely having cash flow issues because of the incident. These costs are still ongoing now, months after the initial incident, and so supplemental reports and related extra administrative burdens would likely be mandated for many months.

We understand that one goal is to be able to determine how many organizations are affected by specific incidents, how those incidents affect different organizations differently, whether analysis shows trends or other actionable analysis for specific types of organizations and/or incidents, and so on, but we question whether the significant added burden on those organizations combined with the absolute glut of reporting that CISA would be getting to review is really needed to meet the intent of the CIRCIA law and if the information gained would be worth the effort expended on all sides.

We do not necessarily have a magic answer here, but certainly as much of the report obligation as possible should be moved closer to the source of the incident. In many cases, the organizations affected by this particular incident use a vendor who uses a vendor who uses Change Healthcare so they didn't even know they would be affected until stuff stopped working for them. Perhaps there is a way to leverage the chain of vendors to get some or all of the required data in a way that limits the report requirements for the healthcare providers, payers, and other unsuspecting users, especially those several steps removed from the original incident source.

Separate and apart from reporting, two things that could be separately mandated (likely outside of this rule) that might help are the following:

1. A disclosure requirement all the way up and down the chain for vendors used by organizations under contract. That is to say, when organization A signs a contract with organization B to provide service X, organization B is required to disclose all of the other organizations involved in providing that service (this would need to be recursive in order to work)
2. A requirement for alternate connection methods so there is no one single point of failure if a vendor like Change Healthcare goes down (for any reason). This phrasing is somewhat specific to the role of Change Healthcare, but general requirements around backups, redundancy, and risk management planning should be in place that consider how any outage at any point in the chain would affect things

The Change Healthcare incident is an extreme example of the single incident impacting multiple covered entities case, but participants in our Data Governance Collaborative note that it is not uncommon for multiple covered entities to be impacted by an incident that occurs in systems they do not directly operate; for many organizations this is more likely than experiencing a direct attack given that incidents at health IT vendors or other third party organizations will likely have a larger effect than incidents directly impacting their customers individually. Thus, a more efficient and effective solution for reporting these types of increasingly more common incidents is likely needed.

## Guidance on Calculating Costs of an Incident

We believe this rule should provide more specifics about what to include in the calculations regarding the cost of a cyber incident and how to calculate those costs. It is easy to determine actual fees paid to mitigate ongoing incidents, but are all internal employees supposed to track time and have their salaries included in the costs? Are lost revenues from the inability to develop new revenue-generating things because those resources were spent on the cyber incident supposed to be tracked and, if so, how? What about lost interest on revenues that were delayed while systems were down? And so on.

Without some sort of consistent rules and expectations, there is no useful way to calculate or compare the

costs of cyber incidents writ large, and the value of collecting this information – likely time consuming and expensive to calculate – is minimized.

### Use of Substantial, Significant, and Similar Terms

Our Data Governance Collaborative notes that this rule frequently uses terms like substantial or significant without a clear definition of what they mean. While in some cases, such as what qualifies as a substantial cyber incident, there are some minimum thresholds laid out, even they rely greatly on judgement calls and interpretation that could legitimately be applied differently by different organizations even when all are acting in good faith. We urge CISA to be explicit whenever possible, and to provide as much guidance as possible (such as that minimum floor criteria) when it cannot.

## Response to Specific Questions

This section will list specific questions asked in the proposed rule and our responses to them.

### 6. Anticipated challenges for covered entities related to understanding or reporting a covered cyber incident if such incident stemmed from a disruption of a third-party vendor or service provider that is itself not a covered entity.

Participants in our Data Governance Collaborative note that there may be significant challenges in meeting reporting requirements when a covered entity uses third parties/vendors to perform or host health IT functions. Among other potential difficulties, they specifically point out:

- Challenges around modifying existing contracts that have already been agreed to by both sides so vendors are required to provide the information needed for CIRCIA reporting that only they have
- Challenges around how to obtain, interpret, and analyze data from organizations that each use their own data structures and storage mechanisms different from other organization's choices for similar data and who may not wish to share data they consider proprietary or that may negatively impact their own business operations
- Challenges around a "not my problem" mentality if the third party vendors are not required to report or otherwise directly interact with CISA regarding CIRCIA

In addition, our Change Healthcare Incident comment above touches on what reporting requirements may be reasonable for covered entities suffering from incidents stemming from third parties, particularly when that third party incident affects multiple covered entities.

### 7. As noted in the preamble, CISA believes there is value in CISA receiving reports on all types of cyber incidents that meet the substantial cyber incident impact thresholds, regardless of whether the TTPs used are sophisticated or not, or novel or not. Therefore, CISA proposes that the "sophistication or novelty of the tactics" should not influence whether an individual incident or category of incidents qualifies as a substantial cyber incident. Do you agree with this proposal, or should the sophistication or novelty of a tactic influence whether an individual incident or category of incidents meets one of the substantial cyber incident thresholds? Similarly, should CISA use sophistication or novelty of a tactic as a justification for including or excluding any specific categories of incidents from the population of cyber incidents required to be reported?

In general, we agree with the approach that the sophistication or novelty of the tactics used in a cyber incident should not drive whether it needs to be reported. However, we do believe that zero-day vulnerabilities should be considered special cases and always be reported (note that we had one contrary opinion, supplied outside

of our interactive discussions, that felt this would be overkill and overwhelm the system). See our comment below for more on this.

## 8. Should exploitation of a zero-day vulnerability as a general matter be considered to meet one of the threshold impacts in the definition of substantial cyber incident? Please provide data or information specifically regarding (1) whether exploitation of a zero-day vulnerability provides an indication of a malicious actor's sophistication, (2) whether exploitation of a zero-day vulnerability results in a different level of risk to a victim entity than exploitation of a known vulnerability, and (3) benefits that reporting on the exploitation of zero-day vulnerabilities might provide to CISA's understanding of the cyber threat landscape, CISA's ability to warn entities about emerging threats, and the federal government's awareness of victim entities targeted in cyber incidents utilizing zero-day vulnerabilities.

Participants in our Data Governance Collaborative note that many of the more impactful incidents in the healthcare sector have come from exploitation of zero-day vulnerabilities and from entities not applying patches to software they use when patches become available (including the recent Change Healthcare incident discussed above, which was caused in part by a vulnerability in unpatched remote access software that was a known vector for attacks). Further, once a zero-day vulnerability is discovered and exploited, it is often a vulnerability in many other systems unless or until a patch fixing it is widely available and applied. Thus, if even a minor incident resulting from a previously unknown or unfixed zero-day vulnerability is reported, that report could prevent many other more significant incidents from occurring by being the catalyst for patch development or for indicating the need for wider promotion of patch availability/the importance of applying a related patch.

As such, they suggest that, contrary to CISA's current plans in this area, requiring reporting of incidents resulting from zero-day vulnerabilities may be warranted regardless of the severity/impact of the incident by other measurement criteria once the cause of the incident is known to be a zero-day vulnerability. Specific suggestions include reporting on whether relevant patches were available at the time of an incident, whether they had been applied, and if not applied, how long they had been available/whether any pre-application testing was underway.

## 17. The scope of entities that would and would not be considered covered entities based on the three criteria proposed by CISA, whether the scoping is appropriate, and what, if any, specific refinements should CISA consider related to any of the criteria.

## 18. The proposal to forgo including specific criteria focused on health insurance companies, health IT providers, and entities operating laboratories or other medical diagnostics facilities.

## 33. The proposed sector-based criteria used in the Applicability Section to identify certain entities as covered entities.

Our Data Governance Collaborative reviewed the criteria specific to the Healthcare and Public Health sector and feels some adjustments would be prudent.

First, while it is likely most payers would meet the size criteria, not all of them do and the loss of a payer would significantly disrupt care for all patients using that payer. Further, depending on the portion of patients under a particular provider's care using that payer, the temporary loss of revenues from a payer can cause significant disruption to the ability of a provider to successfully operate and meet its ongoing financial obligations. Thus,

we believe payers are just as much part of the healthcare sector's critical infrastructure as providers and should be treated as such.

Secondly, we note that neither medical device companies nor pharmacy benefit managers are listed as part of the entities considered part of the Healthcare and Public Health sector. We believe both should quality and should be subject to this rule as entities in one of the 16 critical access sectors should they meet the size threshold or other requirements (we note that certain medical device companies are called out in the sector-specific rules so that aspect is already covered).

Third, we note that the size of a health IT developer/vendor Is often not commensurate with the impact it has in the industry. Software can be developed, tested, and sold with a relatively small number of people involved and some small vendors may fill large roles in the health IT ecosystem. We believe that all health IT developers/vendors, regardless of size, should be covered by this rule. We know that in some cases, their incidents will also need to be reported by other covered entities (see our Change Healthcare comment above), but even if that's the case, the central data around the incident, how it occurred, and how to prevent future similar incidents clearly lies with the entity that was directly affected – the health IT developer/vendor. Regardless of whatever other reporting is received from users of the affected systems, without the core reporting from the directly affected entity reconstructing the incident or learning much of value from a prevention standpoint is likely not possible.

As a general note, CISA notes that one reason they did not explicitly include some of the organizations above was the belief that most cyber incidents affecting them are data breaches and those are not the main focus of CIRCIA. However, in our experience, when a breach of any sort occurs, the affected entity often closes all external connections as a protective/cautionary measure and the entire business is disrupted for a time until the entity is confident it is safe to reopen their connections to the outside world. Thus, while data breaches may not be the major focus of CISA for this rule, they do affect the ongoing ability of an entity to conduct normal business until either investigation has been completed or any potential issues/vulnerabilities/risks beyond data loss are mitigated.

## 31. The proposed decision to include a size-based criterion.

We believe that, in many cases, a size-based criterion makes sense, but CISA should be cautious about applying it universally as there are many types of organizations that fill an outsized role with a small number of employees or with relatively small revenues compared to those of larger corporations doing other types of business (see our comment about health IT vendors above). This becomes a balancing act between burden vs benefits of reporting, including the likelihood of outsized impact.

## 34. Any additional sector-based criteria that would be necessary to capture entities who are only considered covered entities because of the size-based criterion if the size-based criterion was removed the Final Rule.

If the general size-based criterion was removed, we believe the majority of entities in the Healthcare and Public Health Sector SSP list should be covered by this rule, as well as medical device manufacturers and pharmacy benefit managers.

## 50. The establishment of the FISMA reporting exception.

In general, we support this exception with a data sharing agreement that allows CISA access to information about the incidents that otherwise would have been covered by CIRCIA.

## 52. The proposed use of a web-based form as the primary means of submission of CIRCIA Reports

We approve of standardized, structured data and believe this is likely the best way to ensure relative consistency to allow better analysis. We did receive one comment (outside of our interactive discussion) that indicated concern that a web-based form would not be scalable enough to support the level of reporting this rule is likely to generate (see further related comments below).

## the proposed maintenance of telephonic reporting as a back-up reporting option

We approve of this as a backup only, with the expectation that someone is entering the reported data into the web-based system on behalf of the caller and the mechanism of reporting is noted in the provenance of the entered data.

## the possibility of allowing automated ( *i.e.,* machine-to-machine) reporting or other manners of submission in the future at the discretion of the Director.

Participants in our Data Governance Collaborative were confused by this option, believing it the most likely to be compromised/inaccessible immediately after a cyber incident. In general, organizations shut down any and all of their direct external connections after experiencing a cyber incident and thus direct machine-to-machine access would likely be forbidden. Further, it seems somewhat dangerous to allow, let alone encourage, this until such time as a covered entity is absolutely certain there are no residual artifacts of an incursion that could potentially be spread to other systems should a connection be allowed.

We note one contrary opinion, supplied outside of our interactive discussions, that believes a continuous integration pipeline for reporting cyber incidents would be helpful because “these types of incidents as described, happen every day, sometimes multiple times a day” so having to report them individually via a web form would not be sustainable.

## The proposal to use a single, dynamic, web-based form for the submission of all types of CIRCIA Reports, regardless of whether the report is submitted by a covered entity or a third party on the covered entity's behalf.

We support this. There is no reason to have different reporting mechanisms depending on whether an incident is reported directly or via an approved third party.

## 54. The content CISA is proposing be included in all CIRCIA Reports and the specific proposed content for Covered Cyber Incident Reports, Ransom Payment Reports, Joint Covered Cyber Incident and Ransom Payment Reports, and Supplemental Reports, respectively, as well as additional content CISA is proposing to require when a third-party submitter is used to submit a CIRCIA Report on behalf of a covered entity.

In general, we approve of the requested content, although we have some additional suggestions in our zero-day vulnerability comment above and it may be worth considering whether there are other types of incidents that may warrant type-specific additional data requirements.

We also wonder if some of the requested information might be further refined into more granular structured data to better categorize and analyze results. For example, while some ability to provide descriptive content is clearly needed, the basic details of a report could be reported via a set of specific enumerated value lists (always offering other and/or N/A options) supplemented by the longer text description.

## 56. The proposed CIRCIA Report submission procedures, to include the process for notifying CISA that an incident has concluded and been fully mitigated and resolved.

There could, perhaps, be a bit more clarity on the specific requirements around considering an incident resolved. Does that mean analysis complete? Mitigation efforts for future incidents complete? An expectation that no new information will be obtained regardless of current state?

## CISA seeks comments on its proposed approach to enforcement and noncompliance

It is unclear how many of these enforcement actions would be public. Presumably subpoenas are public

documents, but are RFIs also made public or are they private? What about acquisition, suspension, and debarment procedures? Clarification on what can be expected on this front seems warranted. We suggest that differentiating between the existence of an action versus the specific contents may make sense here (i.e. the existence of X being public or private versus the contents of X being public or private) and that the existence of enforcement actions should be public if possible whereas their contents likely should not be in many cases, or should not be without redactions per the information protections outlined in the proposed rule.