OCHIN

A driving force for health equity

Transmitted via online portal

March 13, 2023

The Honorable Richard Hudson
U.S House of Representatives
Washington DC

The Honorable Anna Eshoo
U.S. House of Representatives
Washington DC

Re: *Pandemic and All-Hazards Preparedness Act (PAHPA) 2023 Reauthorization*

Dear Representatives Hudson and Eshoo,

On behalf of OCHIN, we appreciate the opportunity to provide recommendations to strengthen the nation's preparedness for and response to future pandemics or disaster events. OCHIN is a nonprofit national health information technology innovation and research network that is comprised of **locally controlled community-based providers at more than 1,000 health care sites with 22,000 providers in 47 states, reaching more than 6 million patients**. OCHIN has gained significant experience providing rapid technical and operational support to our members during the COVID-19 public health emergency and weather-related regional disaster events as well as assisting members in meeting cybersecurity challenges. With this lens, we urge Congress to amend the current Pandemic and All-Hazards Preparedness Act (PAHPA) and subsequent reauthorizations to authorize and directly appropriate funding to ensure that community-based providers and their health IT networks serving rural and other underserved communities are eligible to lead and develop, and invest in disaster and recover preparedness capacity, planning, sentinel activities, and mitigation activities to meet the specific needs of their patients and communities.

OCHIN Network Addressing COVID-19, Regional Disasters, Cybersecurity

Since its inception over 22 years ago, the OCHIN collaborative of community providers has focused on expanding access in underserved and rural communities to quality health care services through technology solutions, technical assistance, operational support, informatics, evidence-based research, and workforce development and training. Today, the OCHIN network includes federally qualified health centers (FQHC), FQHC look-alikes, rural health clinics, local public health agencies, corrections, school-based clinics, tribal health organizations, youth authorities, and rural hospitals.

- During COVID-19, OCHIN, with limited resources and no advance pandemic disaster planning or mitigation funding, supported our network members by rapidly scaling telehealth capabilities and technical assistance among member provider organizations including in frontier communities and took a leading role[1] along with the CDC and other partners to rapidly develop and implement electronic case reporting[2] (eCR).

[1] Automating U.S. Public Health Reporting to Aid COVID-19 Response, OCHIN Blog, https://ochin.org/blog/automating-us-public-health-reporting-aid-covid-19-response
[2] COVID-19 Electronic Case Reporting for Healthcare Providers, https://www.cdc.gov/coronavirus/2019-ncov/hcp/electronic-case-reporting.html

- OCHIN developed a host of scalable COVID-19 vaccine support tools[3] and provided data to the Administration demonstrating that FQHCs were uniquely positioned to vaccinate the hardest to reach patients who faced lack of transportation and other social drivers negatively impacting access.
- OCHIN also played a critical role in developing, testing, and supporting deployment of mobile technology to support de-centralized delivery of care to expand capacity.[4]
- OCHIN has continued to assist in the development of national digital data and technical standards needed for public health IT sentinel and mitigation capabilities while also actively advocating for prioritizing and aligning CDC and the Office of the National Coordinator for Health Information Technology (ONC) digital data and technical standards prioritizing public health needs.
- Finally, OCHIN continues to identify specific policies that should be pursued to "harden" the cybersecurity measures among community-based providers in rural and other underserved communities.[5]

National Health Security Strategy

During a national health emergency, patients need access to digitally enabled, distributed, and de-centralized health care services to meet them where they are in the community.

- As we have seen from COVID-19, "bricks and mortar" sites of care – like hospitals and nursing homes – can become vectors of disease spread. Further during disasters, these sites can become compromised or difficult to reach. When there are centralized models of care delivery revolving around a hospital, like during COVID-19, clinicians in the community setting can be sidelined while clinicians in hospitals and post-acute facilities are besieged with surges and unable to keep pace.
- To advance de-centralized, distributed, and digitally enabled public health capabilities, community-based clinicians must have ongoing federal investment in modernized health IT and technical assistance, national digital data and technical standards for collection and reporting (with reduction in varied state and local reporting requirements), and resources for networks of community providers. Priority should be given to providers in rural and underserved communities with a strong emphasis on networks with capabilities to drive digital communications with advanced technical capabilities.
- Currently, there is only one PAHPA program that OCHIN members could participate in – the Regional Health Care Emergency Preparedness and Response System - which requires partnerships with hospitals. While the program does not require that the hospital participant be the lead applicant, the reality is that hospitals control and drive the structure of such agreements in a manner that is not consistent with a decentralized and distributed need of community providers that allows them to scale capacity to meet national health security strategic goals. Community-based providers that are part of a network such as the OCHIN collaborative would significantly benefit from a program like the Hospital Preparedness Program so that they are able to undertake the necessary planning, recovery preparedness activities and investments, and mitigation comparable to hospitals in their area while leveraging a national network of community providers.

---

[3] Preparing for Safe & Equitable Distribution of a COVID-19 Vaccine, https://ochin.org/blog/2020/12/4/preparing-safe-amp-equitable-distribution-covid-19-vaccine

[4] New COVID-19 Preparedness App Fills Interoperability Gaps For Surge Preparedness, https://ochin.org/blog/covid19apprelease

[5] OCHIN Comments in response to Cybersecurity is Patient Safety, Policy Options in the Health Care Sector, https://static1.squarespace.com/static/5ade0eb85cfd79247926399a/t/638a8e60cb93ad3f6311f31d/1670024801009/Congress+Comments+to+Sen_+Warner+cybersecurity+policy+paper+%282%29+%281%29.pdf

We recommend that Congress amend the Regional Health Care Emergency Preparedness and Response System Program to allow composition of participants/alliances to be limited to community-based provider networks and provider alliances and organizations. This would not preclude collaboration with hospitals in a region but would allow community-based providers to identify the specific and unique needs of their patients and then employ economies of scale to meet the myriad of challenges in their clinics and communities across the nation. This would also expand the pool of organizations and clinicians prepared and able to respond to pandemics and disasters to minimize surges in local hospitals. We also urge the creation of a community-based provider network analogous to the Hospital Preparedness Program for the same reason.

Strategy for Public Health Preparedness and Response to Address Cybersecurity Threats

Providers in community settings need resources to support ongoing public health preparedness and recovery readiness in the event of public health or a disaster by ensuring they can continue to deliver care, access patient health information, and hand-off care rapidly and safely when necessary. All of these critical capabilities require health IT modernization.

- Community clinics have not received significant incentives or resources for health IT upgrades and modernization for well over a decade. Many have legacy systems even though they now need 21st Century capabilities with enhanced cyber tools to deliver whole patient care, move to value-based payment models (which require significant data analytic capabilities), and maintain reporting capacity during a public health or disaster event.
- Cybersecurity is particularly critical during a pandemic/disaster event. Cybercriminals often view such events as an opportunity to exploit health IT system vulnerabilities, particularly among legacy systems that use antiquated security methods.
- Recovery readiness must include ongoing investments in health IT cybersecurity which should include technical assistance, mitigation support, and back-up capacity to ensure that any core capabilities of provider networks are able to maintain or re-establish access rapidly to both patient health information and connectivity with patients through virtual modalities.
- Priority should be given to provider health IT networks that serve rural and underserved communities, so they are able to make immediate investments to harden recovery readiness and cybersecurity. Unlike hospitals that can leverage higher reimbursement rates and additional adjustments such as those available to disproportionate share hospitals, community networks in unserved areas do not have these enhanced resources.

We recommend that Congress prioritize funding for community-based provider networks in underserved, rural, and metropolitan areas to strengthen their core health IT networks. These networks must have sufficient recovery preparedness capacity to safeguard the health and well-being of residents during large scale emergency events which require investments in advance to mitigate impact on safety and health. These investments also reduce catastrophic costs that can accompany lack of prevention and preparedness. The loss of access to health IT systems, particularly during a catastrophic event, will exacerbate adverse impact on patients facing significant health disparities including those in rural and underserved communities that face social drivers of health that multiply adverse impact.

Public Health Situational Awareness and Biosurveillance Network Programs

We recommend directing resources to accelerate national digital data standards used in health care delivery that are equally important for public health sentinel capabilities. This includes advancing

widespread adoption of national digital data and technical standards for demographic and social drivers of health data as well laboratory test digital data results for use in case reporting.

- ONC needs resources to award grants for digital data and technical standard development, testing, and scaling (with technical assistance) for clinician practices. Thus far, industry standards development bodies have not prioritized or resourced the development of such standards sufficiently. These advance important national priorities and reduce duplicative data collection and reporting obligations for local and regional program/payer needs. Situational awareness and biosurveillance are significantly hampered by lack of investments on both fronts.

We also urge increased transparency with regard to the significant funding provided to CDC by Congress for health IT data systems modernization. Many state and local public health agencies continue to have antiquated health IT systems that hamper electronic case reporting, biosurveillance, and the ability to identify emerging outbreaks or identify communities and populations disparately impacted that need tailored public health responses.

Thank you for your leadership and inclusive approach to gathering stakeholder feedback to inform the PAHPA reauthorization. Please contact me at stollj@ochin.org if we can provide any additional information or be of further assistance.

Sincerely,

Jennifer Stoll
Executive Vice President
External Affairs