“Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack”

Questions for the Record – Dr. Adam Bruggeman

Attachment — Additional Questions for the Record

The Honorable Nanette Barragán

1. Unlike large hospital systems that operate with large financial reserves, physician practices operate on slim margins – especially those who serve our most vulnerable including pediatricians and Medicaid safety net physicians. After the cyberattack, many practices were unable to meet payroll for their operations and nursing staff, pay rent, or order new supplies. What recommendations do you have to support physicians who are still struggling to bounce back?

Response:

When the cyberattack caused Change Healthcare to shut down, it affected all practices’ ability to send claims early in the life cycle and forced physicians to hold claims in the billing bucket until alternative clearinghouse connections were established. Congress and HHS must pursue multiple avenues to support physicians including:

1. **Continuing to provide loans for those physicians and practices still in need.**
CMS could continue providing loans to physicians and practices still in need by extending existing loan program timeframes, increasing loan funding levels, adjust loan terms, simplifying the application process, or providing targeted, proactive outreach to ensure the right mixture of physician groups or practice types/locations still in need.

2. **Ensuring that physicians will not be held financially responsible for damages sustained by their patients from the cyberattack;**
Physicians could be shielded from liability for patient damages resulting from a major cyberattack through measures such as safe harbor laws, regulatory waivers, and clear delineations of responsibility. Safe harbor laws could exempt liability and regulatory penalties for physicians if a cyberattack compromises healthcare data systems out of their control.

3. **Empower CMS and HHS to quickly deploy financial lifelines to physician practices in the wake of a future cyberattack or other emergency that inhibits cash flow.**
Congress could authorize dedicated emergency funding pools or line-items that CMS and HHS can quickly access and disperse during qualifying disruption events. This could involve creating new programs modeled after existing disaster relief funds but tailored specifically for ensuring continuity of care revenue for physician practices. Regulations could also be put in place that allow HHS/CMS to temporarily waive certain requirements and streamline the application and approval processes for providers to receive emergency loans, grants, or advance payment programs when cash flow is disrupted. This would cut red tape to rapidly deploy funds. Finally, Congress should clarify the agencies’ authority to respond to future disruptions so that impacted parties do not lose precious time waiting for guidance.

4. **Remove barriers preventing electronic health records from entering contracts with multiple clearinghouses**
   Electronic health records (EHRs) face several barriers that prevent them from easily entering contracts with multiple clearinghouses. These include proprietary interfaces and integration challenges, as many EHR vendors have requirements that make seamless connections to clearinghouse platforms complex and costly. Exclusivity clauses in some EHR-clearinghouse contracts prohibit the clearinghouse from integrating with competing EHR systems, limiting providers' ability to switch connections. Clearinghouses also often require lengthy, duplicative certification and approval processes for EHR integration. Additionally, the pricing models and fee structures between EHRs and clearinghouses can disincentivize multi-clearinghouse connections, such as higher transaction fees for non-preferred partners. Moreover, there are limited incentives or mandates for enabling easy switching between clearinghouses, and a lack of universal interoperability standards to facilitate seamless data exchange across different platforms.

2. I am concerned that in the aftermath of the recent cyberattack, patients may receive incorrect bills that show they are liable for a larger payment than is appropriate. What steps are being taken to process claims correctly and efficiently?

   Response:

   The cyberattack on Change Healthcare resulted in a complete shutdown, disrupting the ability of all practices to send claims early in their life cycles. Physicians were compelled to hold claims in the billing bucket until alternative clearinghouse connections were established. As a response, efforts are being made to manually log in through payer portals to clarify payments and collaborate with banks to manually clear outstanding payments. However, this undertaking is proving to be extremely time-intensive and lacks funding, posing significant challenges to the affected entities.

3. The systems to facilitate prior authorization requests have been disrupted as a result of the Change Healthcare cyberattack. How has this disruption to prior authorization impacted patients' ability to receive timely care?

   Response:

   Fortunately, many practices conducting surgeries had alternative procedures in place to complete prior authorizations, albeit requiring extended periods and additional staff resources, including overtime work. In line with common healthcare challenges, physicians shouldered these responsibilities, resulting in increased costs as a service to their patients. In our experience, there was limited impact on prior authorization timelines for surgery. However, reports emerged of patients encountering difficulties in receiving pharmaceutical authorizations, leading to heightened out-of-pocket costs and, in some instances, failure to fill prescriptions due to cost constraints.