

WRAP-EM

Western Regional Alliance for
Pediatric Emergency Management



Cybersecurity - Did You Know?

The [Western Regional Alliance for Pediatric Emergency Management \(WRAP-EM\)](#) was founded with the goal of developing a “coordinated, collaborative and sustainable regional pediatric disaster planning and response capability.” With the COVID-19 global pandemic, WRAP-EM recognizes the use of telemedicine has exponentially increased in healthcare organizations across the nation. While COVID has necessitated the increased use of digital care, securing patient data has become increasingly complex. WRAP-EM has identified cybersecurity as a core factor in delivering safe and effective virtual healthcare services. The United States Department of Health and Human Services (HHS) 405(d) Task Group has published the following cybersecurity guidelines within a healthcare environment:

Top 5 Current Threats According to the [Health Industry Cybersecurity Practices \(HICP\)](#):

1. E-mail Phishing Attack
2. Ransomware Attack
3. Loss or Theft of Equipment or Data
4. Insider, Accidental or Intentional Data Loss
5. Attacks Against Connected Medical Devices That May Affect Patient Safety

WRAP-EM is working to identify new security threats – particularly in pediatric emergency events – as telemedicine expands. WRAP-EM has determined that cybersecurity is an overarching issue, recognizing the need for interoperability and collaboration between existing systems and organizations to minimize security breaches. With telemedicine expanding at a rapid pace, healthcare organizations must consider how new technologies introduce novel security threats. As an example, a relaxation of regulations on virtual care due to COVID can exacerbate the impact of cybersecurity in healthcare. To safely protect patient information, providers, and organizations during a major emergency event, WRAP-EM recommends the following questions be considered:

- Is your telemedicine program properly secured in the event of an emergency?
- How is pediatric patient data being transmitted?
- How are they protected and shared among parents/guardians?
- How will patients be safely traced during patient movement?
- Are new technologies and devices FDA approved and/or HIPAA compliant?
- Is your organization’s infrastructure prepared for a telecommunication/power outage or breach?

Telemedicine will continue to expand as legislation adapts to the current landscape. This will introduce new threats with evolving healthcare technology. As the western state regional lead on pediatric disaster and emergency preparedness, WRAP-EM will continue to foster interoperability between organizations and encourage health cybersecurity practices to protect healthcare organizations, professionals, and patients.