POLICY PAPER: DATA SECURITY & PRIVACY

Background

Patient data has become increasingly valuable to cybercriminals because it is a complete, comprehensive data collection. Providers require the utmost security to comply with the Health Insurance Portability and Accountability Act (HIPAA) and protect patients’ sensitive information. The speedy evolution of healthcare IT makes data security a constantly moving target, with methods of protection struggling to stay in front of attack efforts.

The Facts

- Increased use of the electronic health record has created a constant threat of a data breach. Security breaches of the healthcare industry open millions of patients to risks of fraud and identity theft, and can sometimes leave entire healthcare facilities out of commission during an attack.

- As virtual care grows, more openings are created for data breaches to occur because of increased data transfers between patients and providers, and smaller electronic health record (EHR) networks which create duplicates of patient data as opposed to maintaining a single record in the national framework.

- Many of these breaches come in the form of phishing emails, a cyberattack method which is difficult to monitor and prevent. Employee education and engagement makes the best method of prevention of this type of infiltration.

- Healthcare entities require a delicate balance between ease of data utilization by clinicians, nurses, and data analysts, and security and privacy of information.

- Data safety requires a combination of ever-evolving administrative, physical, and technical safeguards to ensure confidentiality of electronic health information, regulated by HIPAA. HIPAA requires physical, network, and process security measures for protected health information.

OCHIN Supports

- Use of the vendor-based, interoperable national framework for electronic health records as opposed to a regional or local health information exchange organizations (HIOs) to prevent copies of patient records which result in higher vulnerability.

- The establishment and implementation of strict security measures before new virtual care methods are brought to the market.

- Programs that subsidize cyber-security defense mechanisms for smaller healthcare providers and federally qualified health centers.

- Expectations that every healthcare provider has security policies, processes/procedures, implementation, measures, and management and oversight.

Questions?
Contact Jennifer Stoll @ stollj@ochin.org