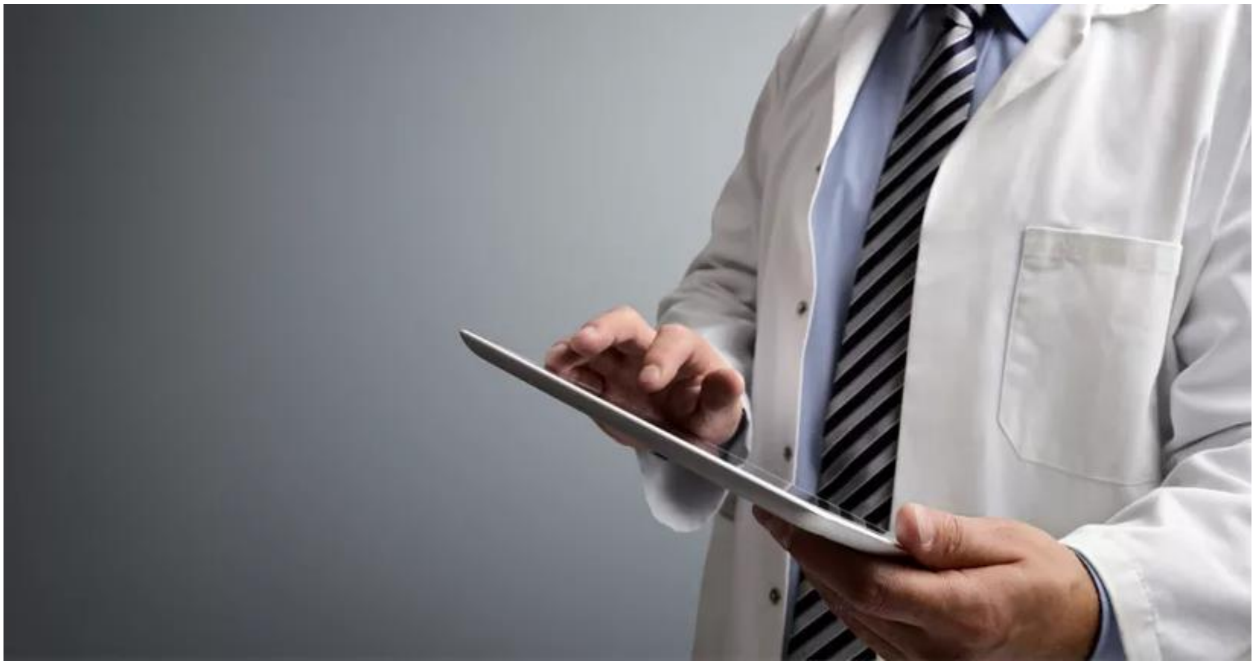
Data Protection for Federally Qualified Health Centers (FQHCs): Focus on Disaster Recovery



July 24, 2018 / Dave McCrystal

In the last few years, Federally Qualified Health Centers (FQHCs) have all upgraded to electronic health records and made steady technical advancements to improve patient care. As they operate in an increasingly competitive environment, the need for cost-effective business strategies and technologies has grown. Consequently, FQHC's are adopting cloud communications capabilities (see video case study) and looking to the cloud for computing solutions like hosting and disaster recovery.

In the days of paper charts, it wasn't necessarily important that systems were up all the time, but it's completely different now in the world of EHRs. Today, if something happens to an FQHC's local facility, they need to get to their data back quickly – via a sound disaster recovery capability – or the quality of care suffers.

FQHCs needs to manage four key components when creating a reliable disaster recovery capability:

1. **Cost** – If companies have local servers, every three to five years they have to go through a process of refreshing this hardware. That cost goes away when using a managed service provider. The fact that you have expandable capacity means you can easily grow your footprint at any time to accommodate increased demand.
2. **Accessibility** –We're in a competitive world now with electronic health workers. In the FQHC market, I need to get to my patient chart wherever I happen to be. If I'm at the coffee shop or at the library, I need to able to get to that patient chart now. A managed service provider has multiple internet service providers, so no matter what you can still get into the system and securely access patient records. Anywhere, anytime access becomes a reality.
3. **Availability** – Uptime means being able to get to your data, and the goal is 100% of the time. We are now in an age where treating patients requires availability. If data access were to go down at any time (whether it's in a disaster scenario or just a normal hardware or software failure in

the datacenter) data needs to be up and available as close to 100% as possible. Managed disaster recovery and hosting solutions provide service level guarantees that FQHCs can rely on to maximize availability.

4. **Security** – Security is perhaps the most critical component. Under HIPAA and meaningful use/HITECH, data must be protected from a security standpoint but also encrypted at a storage level. Protecting “data at rest” means protecting PHI wherever it is sitting, and that it needs to be encrypted, whether it’s on a server, a desktop, or on a laptop. Security needs to be clear and demonstrable, or else you’re potentially sacrificing incentive dollars and/or failing your security assessments. Evolve IP’s HITRUST certification provides assurance to FQHCs that solutions based on our infrastructure were built on a solid, secure, state-of-the-art foundation that clearly meets HIPAA/HITECH standards.

As with every other health center or hospital, Federally Qualified Health Centers are driven by the need to meet HIPAA requirements. But even if HIPAA wasn’t there, there would always be the need for data protection and business continuity solutions to help protect patients information and ensure high-quality care. As time goes on, compliance requirements will undergo continual change, and new threats will emerge. Regardless, Evolve IP is flexible and able to grow in response to FQHC’s needs.

For more information or case studies about Evolve IP’s solutions for healthcare, or details about our HIPAA compliant, HITRUST-certified infrastructure, visit our Healthcare Solutions page.