The Privacy and Security of Your Data is Our Concern

Thousands of independent practices in all 50 states trust GPN technologies, including EDGEPro™ to manage their data in the cloud - and we take this trust very seriously. So many practices are not even aware that their data is being mined by companies for resale, often without the practice's authorization or knowledge of how their vendor is using their proprietary data! Our top priority is to ensure that your practice- and patient-related data remains secure and confidential, and we adhere to the highest professional privacy and security standards to do so. To keep our environment secure, we constantly focus on maintaining the reliability of our product, infrastructure, technologies, and procedures.

GPN currently meets or exceeds the national standards for HIPAA compliance. We regularly and vigorously review our privacy and security policies, procedures and protocols. Then we test, update and test them again - because there is no such thing as "too secure" when it comes to your patient data. We've included questions at the end of this paper that you should be asking *any* company when you are considering granting them access to your practice server.

Certified Partnerships

GPN works hand-in-hand with your Practice Management Software to prevent unauthorized disclosure of your data. We maintain HIPAA-compliant, mutual Business Associate Agreements (BAAs) with each of our integrated software partners, and keep abreast of important regulatory updates. This protects all parties involved. Our client BAA is also available to our end users and may be downloaded at any time from our website, or you may request a copy of this document from our Client Services Department.

Our Policies Protect Your Data

Advanced Encryption Standard. All transmissions between practice servers and EDGEPro™ servers are encrypted with industry standard software, and transmitted across secure connections. We test quarterly and upgrade server certificates annually to ensure only the most current, bit-strength encryption standards and ciphers are allowed.

Independent Security Reviews. All GPN technologies, their systems, servers, and encryption methods are subjected to regular security penetration tests by an independent 3rd party security firm to ensure no vulnerabilities exist to malicious or unauthorized outside access. GPN retains specialized legal counsel to review our compliance policies, assist with our annual employee compliance training, and ensure that we are always following current requirements and industry best practices for security.

Access Restriction. Access to your data is tightly restricted. Only those GPN employees who require it in order to perform their specific job functions are granted access, and even those employees are given the absolute minimum needed to perform their jobs. Password-protected entry is mandated for all EDGEPro™ users, including our employees.

Employee Training. Every member of our team lives and works in the U.S. and undergoes robust HIPAA training. They must demonstrate their understanding of HIPAA before they are granted access to EDGEPro™ platform. Additionally, new information and policy reviews are disseminated to the GPN team as they become available and on an annual basis.

Continuous Review and Improvement. GPN is constantly improving and tightening its security policies. Because digital environments and operating systems are constantly changing, it is imperative that our development and application team stays up-to-date with the latest platform versions and potential threats. We work just as hard to continuously improve your user experience with new features and information options.

Account Security. Last, but not least, we use the most current techniques to protect your data at the user level. Access to any EDGEPro™ account is granted only by password-protected logins over encrypted connections.

Auto-Log Out. "Inactive" users are timed out automatically to prevent accidental exposure on shared work stations, and all passwords are encrypted and masked completely, meaning they never appear in readable plain text. Your passwords are not even visible to our team members on any level.

We Value Your Trust

We recognize and deeply appreciate the trust you place in us as your chosen analytics provider. You can take comfort in the knowledge that we will continue to proactively guard our systems – and your data – with your privacy and security in mind.