Professional
Data Analysts

655 19th Ave NE, Suite 100
Minneapolis, MN 55418
612.623.9110

Technology and Process for Securing Information

Data security and integrity is very important in our day to day business at PDA. PDA stores, shares, and analyses sensitive data every day and uses a variety of procedures, methods, and guidelines to ensure data confidentiality and integrity.

DirectTrust

PDA is authorized and qualified to send and receive secure health information via the DirectTrust network. The DirectTrust network is a well-established, ANSI-accredited, standardized network of secure data transmission partners (HISPs) which meet very strict security and industry standards. PDA utilizes EMR Direct, one of the founding members of the network as their HISP to send and receive sensitive data. Members of the DirectTrust network are required to conduct regular audits and validate compliance of well-established healthcare industry standards.

Federal standards

PDA also adheres to the rules defined in NIST Special Publication 800-53 and Federal Information Processing Standards Publication 200 including, but not limited to, the following:

Access controls on information systems

Access to information on PDA's information system is protected by access controls through Microsoft Active Directory (AD). Through AD, users are identified by username, authenticated via password, and authorized to access only the data required to complete specific tasks.

Firewall protection

Internet and remote access to PDA's services are protected by an advanced firewall. The firewall uses both stateful and stateless techniques to prevent malicious packets from entering PDA's internal network.

Encryption of data while in motion

All data in motion in encrypted at PDA. Internet access is automatically redirected to HTTPS via a reverse proxy server. The reverse proxy handles external as well as internal internet requests. Remote access to data servers is encrypted by IPsec and SSL based VPNs.

Encryption of data at rest

Data at rest on PDA's servers is protected via self-encrypting disks using 256-bit encryption.

Data at rest on PDA's laptop and desktop computers is protected by Bitlocker using 256-bit encryption.

655 19th Ave NE, Suite 100
Minneapolis, MN 55418
612.623.9110

Disaster recovery procedures

PDA has a written disaster recovery procedure with contingency plans including power outages, hardware failure, and data loss events. The procedure details the tasks and responsibilities of staff at PDA to mitigate the effects of any disaster.

Staff training

Staff security training at PDA happens at regular intervals and includes exercises on phishing attacking, social media exploits, and fraudulent emails. Initial hire training also includes navigating physical access controls, password policies, reporting policies, and HIPAA data related training.

24/7 security monitoring

Physical monitoring of PDA's office is accomplished using a sophisticated access control system. Employees are provided key fobs that only allow access to assigned areas. All fob usage is tracked and fully auditable. In addition to access control, all doors in and out of PDA's office or sensitive data rooms are under camera surveillance, and the camera DVR stores high definition video for up to 60 days. PDA's office is further monitored by motion sensors connected to a burglar alarm that notifies PDA administrators and the police when tripped.

Redundant offsite backups

PDA maintains fully redundant offsite backups at a colocation. The backups are incrementally updated each night. The physical aspects of the colocation are managed by a third party and verified by a SOC 2 type 2 audit. The infrastructure of the colocation is configured to act as a warm site and is heavily featured in disaster recovery procedures.

Additional standards

Vulnerability testing

PDA conducts quarterly internal vulnerability tests. The internal test checks for common configuration and security issues inside PDA's network. Additionally, PDA contracts a third party for an annual external vulnerability test. The external test attempts to access unauthorized data on PDA's server through the firewall via the internet. All identified issues are resolved within 90 days.