HIPAA Compliance Information

Saved From: http://support.vridirect.com/article/hipaa-compliance-information-25.html

VRI Direct is a HIPAA-compliant VRI platform that follows best practices in the storage and accessibility of protected health information (PHI) both at rest and in motion. The following is a description of what HIPAA requires, how it relates to VRI Direct, and what VRI Direct does to maintain HIPAA compliance.

HIPAA Privacy Rule
The Privacy Rule endeavors to protect individuals' health information by preventing the transmission of PHI over open networks or downloading it to public or remote computers without encryption. This rule is often referenced in conjunction with the term data in motion (data that is transmitted across a network, for example).

Because VRI Direct does not ask for any protected health information, nor does VRI Direct record or store audio, video or text chat streams, the risk of transmitting protected health information is low; however, VRI Direct understands the importance of maintaining HIPAA-compliant practices regardless of data type, and has instituted the following measures:

- All network transmissions between VRI Direct servers and VRI Direct users, and across VRI Direct servers, are encrypted. Audio, video and text chat streams are encrypted and transmitted using 128-bit AES and 256-bit SSL encryption. Web request/response actions are transmitted using 256-bit SSL encryption;
- All network transmissions between VRI Direct servers and VRI Direct IT personnel are encrypted using key-based SSH authentication.

HIPAA Security Rule
The Security Rule requires covered entities such as VRI Direct to install administrative, physical and technical safeguards to protect electronic PHI. These safeguards include access controls, data encryption, and auditing in a manner that is commensurate with the associated risk.

Since VRI Direct does not directly ask for protected health information and does not record audio, video or text chat streams, VRI Direct's associated risk is low; however, VRI Direct remains sensitive to implementing practices that meet HIPAA requirements:

- VRI Direct servers are hosted in Amazon's AWS data centers, which are themselves HIPAA-compliant. For more information, please read "Creating HIPAA-Compliant Medical Data Applications with AWS", which includes information about Amazon Web Services's own HIPAA-compliant practices;
- All remote server access is through key-based, encrypted SSH sessions. This access is also audited using server logs;
- Physical server access requires multi-factor authentication (password, card reader, handprint/thumbprint authentication) and is audited;
- Server passwords follow strong password requirements (eight or more characters; no dictionary words; combination of case-sensitive alphanumeric/symbolic characters) that must be reset several times per year (typically every 90 days);
- Server access is restricted to Amazon IT personnel and VRI Direct technical personnel. The VRI Direct personnel access list is audited by the CTO every 90 days. Amazon Web Services employees do not have access to VRI Direct's EC2 instances. AWS employees have access to the VRI Direct database backup servers on S3, but this access is highly restricted and not necessary for VRI Direct support or maintenance. Visit https://aws.amazon.com/security/ for more information;
- Form fields that collect arbitrary data are encrypted with AES-256 encryption prior to storage;

- No audio, video or text chat streams are recorded or stored, either temporarily or permanently, by VRI Direct on any VRI Direct servers.