SECURITY INFORMATION

Data Backup Process:

EZDERM is a cloud-based platform hosted on Amazon Web Services (AWS), the leader in cloud computing. Our servers and databases are backed up on a daily basis. For redundancy, we also take backups of backups in order to take all steps possible to prevent data loss in disaster situations. Individual users are not required to perform backups as the system has been designed to automate the backup process.

Our backups are located in multiple Amazon Availability Zones. AWS consists of one or more discrete data centers, each with redundant power, networking and connectivity, housed in separate facilities. This would help recover data from a single Availability Zone outage, if needed.

Encryption:

EZDERM has encrypted communication via HTTPS with latest TLS protocol, HIPAA compliance, and system monitoring of data security.

Best Practices for HIPAA Security:

- Don't share password with other users.
- Create a complex password (Secure Password Generator) that is changed regularly.
- Deactivate users who are no longer part of the practice immediately.
- Set up Access Permissions according to user roles.
- Logout of account when not at computer or iPad. Do not leave protected health information (PHI) on the screen when not working on that chart.
- Provide up-to-date training program on the handling of PHI for employees performing health plan administrative functions.
- Avoid accessing a patient's record unless needed for work.
- Minimize occurrences of others overhearing patient information. Do not use a patient's whole name within hearing distance of others.
- Never email PHI. If the information cannot be sent another way, use email encryption.
- Always use a cover sheet when faxing PHI.
- Make sure computers have updated anti-virus scanning software installed. This helps guard your practice against malicious software.