Dental Billing Software Access Guide

This guide outlines how Elite Billing Solutions securely connects to your dental software systems, whether they are cloud-based or hosted locally. It helps clients understand what tools, permissions, and security measures are needed for efficient and HIPAA-compliant remote billing.

Cloud-Based Systems

1. Confirm the software is HIPAA-compliant and can be accessed remotely via secure login.
2. Provide user credentials with appropriate permissions (limited to billing as needed).
3. Enable multi-factor authentication if available.
4. Ensure strong passwords and that only authorized staff share credentials.
5. Coordinate a secure messaging channel for sharing login credentials (e.g., encrypted email, password manager).
6. No additional VPN is typically needed for cloud-based platforms.

Local Server (On-Premise) Systems

1. Confirm whether the practice uses Dentrix, Open Dental, Eaglesoft, or another server-based system.
2. Set up a HIPAA-compliant VPN (the practice may provide this, or you can use your own).
3. Use Remote Desktop software approved by the practice for secure access to their server.
4. Ensure that only necessary permissions are granted for billing activities.
5. Work with the office's IT vendor to configure secure, time-limited access if possible.
6. Document login procedures and contacts for IT support in case of access issues.

Security & HIPAA Compliance

1. Never store patient PHI locally unless encrypted and necessary.
2. Use encrypted communication platforms for sharing any PHI (e.g., Paubox, LuxSci, or HIPAA-compliant email).
3. Sign Business Associate Agreements (BAAs) with vendors providing remote access tools if required.
4. Regularly review and update security protocols with each client.

Following this guide ensures a smooth onboarding process and maintains HIPAA compliance when accessing client dental software systems remotely. For any questions or additional security requirements, please contact us.