Best Practice Pointer No. 16
Secure Transmission, Confidentiality, and Cybersecurity

CYBERSECURITY IS CRUCIAL FOR COURT REPORTERS.

Court reporters' transcripts often contain sensitive and/or confidential information that, if exposed, could lead to legal, financial, or reputational harm for individuals or organizations.

Strong cybersecurity practices help:
- Prevent unauthorized access to private data.
- Ensure compliance with legal and ethical obligations to maintain confidentiality.
- Safeguard against cyberattacks such as phishing, ransomware, and data breaches.

It is important to prioritize cybersecurity. Court reporters can maximize efforts to ensure the confidentiality, integrity, and security of their work product by adhering to the following best practices related to cybersecurity:

1. **Keep Operating Systems and Other Software Updated**
   - Regularly install updates for the operating system and other software on all work-related devices to help address security vulnerabilities.

2. **Secure External Storage Devices**
   - Protect all work-related external drives and USB devices with strong passwords.

3. **Protect Mobile Devices**
   - Enable password or passcode protection on your smartphone and other mobile devices used for work.
   - Exercise caution when using a public or unsecured network.

4. **Implement Strong Password Practices**
   - Change your passwords regularly, such as every 90–120 days.
   - Use multifactor authentication (MFA) whenever possible.
   - Create strong passwords that include capital letters, special characters, and numbers.
   - Avoid reusing passwords across different accounts.

5. **Use Antivirus Software**
   - Maintain up-to-date antivirus software on your work computer to safeguard against malware and other threats.

6. **Back Up Files**
   - Ensure all work-related files, including transcripts, are backed up securely, using encrypted cloud services or password-protected drives.

7. **Transmit Data Securely**
   - Use secure methods to transmit transcripts and exhibits, whether shared by you or your support team (e.g., encrypted email or file transfer services).

8. **Ensure Data Integrity**
   - Use secure upload methods/tools to prevent documents from being tampered with during transmission, ensuring the accuracy and reliability of your files.

BEST PRACTICE POINTER SECURE TRANSMISSION, CONFIDENTIALITY, AND CYBERSECURITY

9. Prevent Unauthorized Access

- Use secure methods/tools to ensure that only authorized individuals can view or download sensitive (medical or proprietary) documents, reducing the risk of data breaches.

10. Retention and Destruction of Documents

- Shred/destroy exhibits and documents when instructed to by clients or the deposition firm.
- Develop a retention policy for the eventual destruction of documents.
- Delete scanned copies of all documents, including from all backup sources, when you are finished working with them.

11. Disposal of Electronic Devices

- Take appropriate measures to ensure the proper removal of all sensitive or confidential information from electronic devices before disposal.

12. Maintain Client Trust

- Build trust and confidence with clients by exercising strong security measures.

Following these practices demonstrates that you prioritize the safety of their sensitive information.

Best practice pointers are not regulations or statutorily mandated. They are a way for the Board to provide guidance on situations not expressly set out in statute or regulation. Although the pointers may be used by licensees as a guide, the Board will not use them as a basis for discipline or enforcement of any type.

COURT REPORTERS BOARD OF CALIFORNIA

2535 Capitol Oaks Drive, Suite 230
Sacramento, CA 95833
Phone: (916) 263-3660 / Toll Free: (877) 327-5272
Fax: (916) 263-3664
www.courtreportersboard.ca.gov

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS