Practice-Web Dental Software Security Policy

Effective Date: July 23, 2018
Last Updated: May 8, 2023

Introduction

At Practice-Web, we recognize the importance of maintaining the privacy and confidentiality of patient and practice data. This Privacy Policy outlines how data is managed, protected, and shared within the Practice-Web dental software system, focusing on our commitment to ensuring the security and privacy of data for dental practices using our on-premises, server-based software. As an on-premises solution, Practice-Web operates within the local server infrastructure of each dental practice, meaning that the dental practice itself exercises primary control over the storage, management, and security of patient data.

While Practice-Web provides robust tools for managing data, responsibility for securing this data primarily rests with the practice. However, there are situations where Practice-Web's support team or third-party specialists may handle or access the practice's data to provide services such as troubleshooting, support tickets, or data conversions. This policy outlines how such data is handled to protect privacy, comply with relevant regulations (e.g., HIPAA), and safeguard sensitive information during these interactions.

By using Practice-Web software, dental practices agree to the terms outlined in this Privacy Policy. This policy provides comprehensive guidance on how data is managed, how privacy is protected, and the rights of the practices regarding their data.

Key Definitions

To ensure clarity, this section defines key terms used throughout the Privacy Policy:

- **"Personal Information" (PI)**: Any data that can be used to identify a specific individual, such as a patient or staff member. This includes, but is not limited to, names, addresses, phone numbers, Social Security numbers, medical and dental records, and insurance information.
- **"Protected Health Information" (PHI)**: Any individually identifiable health information that is transmitted or maintained in electronic or physical form. PHI is subject to HIPAA regulations and includes data such as patient medical histories, treatment plans, and diagnostic information.
- **"Data Controller"**: In this context, the dental practice is the data controller, meaning it has full control over how data is collected, stored, and used. Practice-Web acts as a data processor only when necessary (e.g., during support activities).

- **"Data Processor"**: Any entity or person who processes data on behalf of the data controller. In cases where Practice-Web specialists assist with support or data-related tasks, Practice-Web functions as a data processor under the direction of the practice.
- **"On-Premises Solution"**: A software setup where data is stored and managed on servers physically located within the dental practice rather than in the cloud or third-party data centers.

---

1. Data Ownership and Control

1.1 Primary Data Ownership

As an on-premises dental software, all data managed within Practice-Web is stored on local servers located at the dental practice. **The dental practice itself is the sole owner of the data** and has full control over its management, storage, access, and deletion. Practice-Web does not have access to this data unless explicitly provided by the practice for the purposes of support or service requests.

The dental practice retains full ownership and responsibility for patient records, billing information, appointment details, and other practice-related data. This includes ensuring that data is stored securely and backed up regularly. Practice-Web provides the tools and software for managing data, but the practice is responsible for implementing and maintaining the necessary physical and technical safeguards to protect this data.

1.2 Data Responsibility of the Dental Practice

As the data controller, the practice must ensure that it complies with all applicable privacy laws, including HIPAA, which governs the use and disclosure of PHI. This includes:

- **Data Security**: Implementing access controls, encryption, and other security measures to protect data stored on local servers.
- **Access Management**: Limiting access to patient data to authorized users and ensuring that employees understand their obligations to maintain patient confidentiality.
- **Data Retention**: Determining how long data is retained in the system and managing the deletion of old or outdated records in compliance with regulatory requirements.
- **Audit Trails**: Maintaining records of data access and modification to track who has accessed sensitive information and when.

---

2. Data Access by Practice-Web for Support and Maintenance

While Practice-Web is an on-premises solution, there are instances where Practice-Web personnel or authorized third parties may need to access the practice's data to provide services

such as technical support, troubleshooting, data conversions, or upgrades. In such cases, Practice-Web follows strict guidelines to ensure that data privacy is maintained.

2.1 Support Tickets and Troubleshooting

When a dental practice submits a support request (e.g., for technical troubleshooting or bug resolution), it may be necessary for Practice-Web support specialists to access specific data in the system. The following measures are in place to protect the privacy of the data during these interactions:

- **Explicit Authorization**: The practice must explicitly grant Practice-Web access to its system or provide specific data files for troubleshooting. Access is not obtained without prior permission from the practice.
- **Remote Access Protocols**: In cases where remote access is needed (e.g., via a remote desktop connection), all sessions are conducted over secure channels (e.g., Zoho Assist). The practice has the ability to monitor and control these sessions, and access is terminated as soon as the support task is completed.
- **Minimization of Data Exposure**: Practice-Web staff will only access the minimum amount of data necessary to resolve the issue. For example, if a support ticket pertains to billing functionality, access will be limited to financial data rather than patient medical records.
- **Logging and Audit**: All access and activity by Practice-Web staff during support sessions are logged and can be reviewed by the practice to ensure that data privacy has been maintained.

2.2 Data Conversions and Migrations

Occasionally, practices may need to convert data from other systems into Practice-Web, or migrate data from Practice-Web to another system. In these instances, the following guidelines apply:

- **Data Handling During Conversions**: If Practice-Web specialists assist with data conversions (e.g., importing data from legacy systems), the practice will provide specific data files for conversion. These files are handled securely and are only used for the purposes of data conversion.
- **Temporary Access**: Data provided for conversion is only accessed during the duration of the project and is securely deleted or returned to the practice once the conversion or migration is complete.
- **Encryption During Transfers**: If data must be transferred electronically (e.g., via secure file transfer), it will be encrypted using industry-standard protocols (e.g., AES-256) to protect it from interception or unauthorized access during transit.
- **Third-Party Data Processors**: If third-party specialists are involved in data conversions or migrations, they will be subject to the same privacy and confidentiality requirements as Practice-Web staff, and the practice will be informed of their involvement.

3. Data Security Measures

Practice-Web takes data security very seriously, and while the dental practice maintains control over its data, we provide tools and recommendations to help practices secure their systems. Below are the key security measures recommended for practices using Practice-Web:

3.1 Encryption

- **Data Encryption**: Data stored on the server should be encrypted at rest using industry-standard encryption algorithms (e.g., AES-256). Practice-Web supports database encryption to protect sensitive data such as patient records, billing information, and diagnostic data.
- **Encryption of Backups**: Backup data should also be encrypted to protect it in case of theft or loss. Practices should ensure that both onsite and offsite backups are encrypted using strong encryption standards.
- **Encryption of Data in Transit**: When data is transmitted between workstations and the server (or between the server and Practice-Web specialists for support purposes), it should be encrypted using TLS (Transport Layer Security) to prevent unauthorized interception.

3.2 Access Controls

- **Role-Based Access Control (RBAC)**: Practice-Web allows practices to implement RBAC to restrict user access based on job roles and responsibilities. Access to sensitive data (e.g., PHI) should be limited to authorized users, such as dentists, billing specialists, and other relevant staff.
- **User Authentication**: Each user must have a unique username and password to access the system. Practices should enforce strong password policies, including password complexity, expiration, and reuse restrictions.

3.3 Logging and Audit Trails

- **Comprehensive Logging**: Practice-Web logs all user activities within the system, including access to patient records, data modifications, and system changes. These logs are accessible to the practice for auditing purposes and to investigate potential unauthorized access or misuse.
- **Audit Trails**: The software provides detailed audit trails, tracking who accessed or modified specific patient records and when these actions occurred. This feature is essential for complying with regulations such as HIPAA.

3.4 Data Backups and Recovery

- **Automated Backups**: Practices are responsible for configuring and maintaining regular backups of their Practice-Web data. The software supports automated backups to ensure that data is consistently backed up without manual intervention.
- **Offsite Backups**: Practices are encouraged to maintain offsite or cloud backups of their data to protect against data loss due to disasters such as fires, floods, or system failures. These backups should be encrypted and stored securely.
- **Disaster Recovery**: Practices should develop a disaster recovery plan to ensure that data can be restored promptly in the event of a system failure or data breach.

---

4. Compliance with Data Privacy Regulations

4.1 HIPAA Compliance

Practice-Web is designed to help dental practices comply with the **Health Insurance Portability and Accountability Act (HIPAA)**, which sets the standard for protecting sensitive patient data in healthcare. As a HIPAA-compliant solution, Practice-Web incorporates features and safeguards that align with HIPAA's requirements for the protection of PHI.

- **Privacy Rule**: The HIPAA Privacy Rule restricts the use and disclosure of PHI. Practice-Web provides features such as role-based access control and user authentication to ensure that only authorized users have access to PHI.
- **Security Rule**: The HIPAA Security Rule requires practices to implement physical, administrative, and technical safeguards to protect ePHI (electronic PHI). Practice-Web supports encryption, audit trails, and access controls to help practices meet these requirements.
- **Breach Notification Rule**: In the event of a data breach involving PHI, the dental practice is responsible for notifying affected individuals and, in certain cases, regulatory authorities. Practice-Web's logging and auditing features can assist practices in identifying the scope of a breach and determining which records were affected.

4.2 State-Specific Regulations (e.g., CCPA)

Depending on the location of the practice, other privacy laws may also apply. For example, the **California Consumer Privacy Act (CCPA)** provides additional rights to patients located in California, including the right to access their personal information and the right to request that their data be deleted.

Practice-Web supports these requirements by allowing practices to:

- Provide patients with access to their health records upon request.

- Delete patient data upon request, in compliance with the practice's data retention policies and legal obligations.

---

5. Data Retention and Deletion

5.1 Data Retention

The dental practice is responsible for determining its data retention policies, including how long patient records, financial data, and other sensitive information are stored. Practice-Web allows practices to retain data in accordance with legal and regulatory requirements, such as HIPAA, which requires certain records to be retained for six years.

5.2 Data Deletion

Upon request, practices can delete patient data from the system. Practice-Web provides tools for securely deleting patient records and associated data, ensuring that it is no longer accessible within the system. However, practices must ensure that deletion complies with any legal or regulatory requirements that may mandate the retention of certain types of records for specific periods.

---

6. Data Access Rights and Patient Privacy

Patients have the right to access their health records, as outlined by HIPAA and other privacy laws. Practice-Web provides practices with tools to:

- **Respond to Patient Data Requests**: Practices can generate reports containing a patient's health information, including treatment history, billing details, and other relevant records.
- **Update Patient Records**: If a patient requests corrections to their records, practices can update the data in Practice-Web to ensure accuracy and compliance with the law.
- **Provide Data in Portable Formats**: If a patient requests a copy of their records in a portable format (e.g., for transferring to another healthcare provider), Practice-Web allows practices to export records in standardized formats, such as PDF or CSV.

---

7. Privacy Breach Response

In the event of a privacy breach involving patient data, the dental practice is responsible for taking the following actions:

- **Investigation**: The practice should use Practice-Web's audit trails and logs to investigate the scope of the breach and determine which records were accessed.
- **Containment**: The practice should take immediate steps to contain the breach, such as disabling user accounts or restricting access to sensitive data.
- **Notification**: In compliance with the HIPAA Breach Notification Rule (and any applicable state laws), the practice must notify affected individuals of the breach and report the breach to regulatory authorities if required.
- **Remediation**: After addressing the breach, the practice should review its security practices and update any policies or procedures to prevent future incidents.

---

8. Conclusion

Practice-Web is committed to helping dental practices protect the privacy of their patient data while providing the tools necessary for efficient and effective practice management. As an on-premises solution, the primary responsibility for data security and privacy rests with the dental practice. By implementing the security settings, access controls, and data management features outlined in this Privacy Policy, practices can ensure that their data is protected and that they remain compliant with all applicable privacy laws.

For any questions regarding this Privacy Policy or assistance with configuring security settings, please contact the Practice-Web support team.

---

9. Contact Information

For additional information on privacy practices or data handling policies, please contact:

- **Email**: support@practice-web.com
- **Phone**: 1-800-845-9379
- **Website**: www.practice-web.com