HIPAA SOFTWARE COMPLIANCE CHECKLIST

FOR NONPROFITS

1. DATA SECURITY & ENCRYPTION

□ Encrypts data at rest (stored client records and files)

□ Encrypts data in transit (data sent between users and systems)

□ Uses secure, industry-standard encryption protocols

2. ACCESS CONTROLS & USER PERMISSIONS

□ Supports role-based user permissions

□ Allows administrators to control who can see sensitive client data

□ Restricts access to case notes, documents, and health information

□ Enables quick removal of access when staff or volunteers leave

Tip: Nonprofit case management solutions like Sumac are built with HIPAA compliance in mind and meet al 7 of these requirements.

3. AUTHENTICATION & USER SECURITY

□ Includes secure authentication methods (strong passwords, MFA)

□ Prevents unauthorized access through session controls or timeouts

□ Tracks user logins and access activity

HIPAA COMPLIANCE CHECKLIST

FOR NONPROFITS

4. AUDIT LOGS & MONITORING

□ Maintains detailed audit logs

□ Records who accessed PHI, when, and what actions were taken

□ Supports audit reviews for HIPAA compliance audits

5. DATA BACKUP & RELIABILITY

□ Provides automatic, reliable data backups

□ Ensures data recovery in the event of system failure or breach

□ Protects against accidental data loss or corruption

6. VENDOR COMPLIANCE & LEGAL SAFEGUARDS

□ Vendor signs a Business Associate Agreement (BAA)

□ Software is designed to support HIPAA compliance requirements

□ Vendor demonstrates ongoing security and compliance practices

Tip: Generic spreadsheets, unsecured CRMs, or free tools are not sufficient for HIPAA compliance. To protect your nonprofit, opt for a secure case management solution like Sumac.