Tech Integration for Therapists

Clinical Documentation Systems, Practice Tools, and AAMFT Code Section 6 Considerations

---

Introduction

Technology has become integral to modern therapy practice, offering powerful tools for documentation, communication, scheduling, and client care. However, with these benefits come significant ethical and legal responsibilities. This guide provides an overview of clinical documentation systems, essential practice tools, and the ethical framework outlined in AAMFT Code of Ethics Section 6: Technology-Assisted Professional Services[1].

Purpose of this guide:

- Help therapists select appropriate technology solutions
- Understand HIPAA compliance requirements
- Navigate AAMFT ethical standards for technology use
- Implement best practices for secure documentation and communication

---

AAMFT Code of Ethics Section 6: Technology-Assisted Professional Services

The AAMFT Code of Ethics Section 6 establishes ethical requirements for offering therapy, supervision, and related professional services using electronic means[2]. Understanding these standards is essential before implementing any technology in your practice.

6.1 Technology-Assisted Services

Requirements before commencing services:

- Ensure compliance with all relevant laws for delivery of electronic services
- Determine that technology-assisted services are appropriate for clients/supervisees (considering professional, intellectual, emotional, and physical needs)
- Inform clients/supervisees of potential risks and benefits
- Ensure security of communication medium
- Obtain appropriate education, training, or supervised experience using the technology

Clinical implications: Not all clients are suitable for telehealth or technology-assisted services. Consider factors such as crisis risk, cognitive functioning, technology access, and privacy concerns when determining appropriateness[2].

6.2 Technology and Consent to Treat

Written consent requirements:

Clients and supervisees must be made aware in writing of:

- Risks associated with technology-assisted services
- Both therapist's and client's responsibilities for minimizing risks
- Emergency procedures and backup communication methods
- Limitations of technology platforms used

Best practice: Include technology-specific consent forms as part of your intake process, covering telehealth platforms, client portals, secure messaging, and any other electronic communication methods[2].

6.3 Technology Selection and Responsibility

Therapist responsibilities:

- Choose platforms that adhere to best practices for confidentiality and quality

- Ensure technology meets applicable laws (HIPAA, state regulations)
- Inform clients in writing of limitations and protections offered
- Select suitably advanced and current technology

Key considerations:

- Business Associate Agreements (BAAs) required for HIPAA compliance
- End-to-end encryption for video and messaging
- Data storage location and security measures
- Vendor compliance certifications (SOC 2, ISO 27001)

6.4 Technology and Documentation

Documentation security requirements:

All electronically stored or transferred documentation containing identifying or sensitive information must:

- Use technology adhering to best practices for confidentiality
- Meet quality of service standards
- Comply with applicable laws
- Be explained to clients in writing (limitations and protections)

2026 updates: Explicit documentation now required for protecting Substance Use Disorder (SUD) data and reproductive health information, with enhanced protections beyond standard HIPAA requirements[3].

6.5 Jurisdictional Compliance

Therapists must follow all applicable laws regarding location of practice and cannot use technology to practice outside allowed jurisdictions[2].

Licensure considerations:

- Verify telehealth laws in both your state and client's state
- Obtain additional licenses if providing cross-state services
- Understand temporary emergency provisions vs. standard requirements

6.6 Training and Competence

Competence requirements:

- Be well trained in all chosen technology-assisted services
- Make careful choices of audio/video/other options to optimize quality and security
- Ensure technology is suitably advanced and current
- Maintain competence through ongoing education

Training areas: Platform operation, troubleshooting, security protocols, emergency procedures, ethical considerations, and clinical best practices for technology-mediated therapy[2].

HIPAA Compliance Fundamentals

The Health Insurance Portability and Accountability Act (HIPAA) sets the baseline for protecting client health information in the United States. All therapy technology must be HIPAA-compliant[4].

Key HIPAA Requirements

Administrative Safeguards:

- Written policies and procedures for PHI protection
- Annual staff training on HIPAA compliance
- Risk assessment and management plan
- Designated privacy and security officers (may be same person in small practices)

Technical Safeguards:

- Encryption of data in transit and at rest
- Audit logs tracking all access to PHI
- Multi-factor authentication (MFA)
- Automatic logout after period of inactivity
- Role-based access controls

Physical Safeguards:

- Secure physical location for systems storing PHI

- Locked file storage for any paper records
- Screen privacy filters and positioning
- Secure disposal procedures for devices and records

Business Associate Agreements (BAAs):

Any vendor that handles, stores, or transmits PHI must sign a BAA. This includes:

- EHR/EMR vendors
- Telehealth platforms
- Cloud storage providers
- Email encryption services
- Billing and payment processors
- Practice management systems[4]

2026 Compliance Updates

Mandatory risk assessment plan: Therapists must document:

- Where data is vulnerable (mobile devices, backup drives, cloud storage)
- Procedures for handling records requests
- Staff training schedules and completion records
- How sensitive records are protected (SUD, reproductive health, HIV status)[3]

Clinical Documentation Systems

Clinical documentation systems (also called EHR/EMR systems) form the backbone of modern therapy practice, managing client records, treatment plans, progress notes, and billing[5].

Essential Features

Documentation capabilities:

- Customizable note templates (SOAP, DAP, BIRP, GIRP, PIRP, progress notes)
- Treatment planning with goal tracking
- Assessment tools (PHQ-9, GAD-7, PCL-5, outcome measures)

- Crisis documentation (safety plans, risk assessments)
- DSM-5/ICD-10 diagnosis tracking and coding[6]

Practice management:

- Appointment scheduling with automated reminders
- Client portal for secure communication
- Insurance billing and claims management
- Superbill generation
- Payment processing
- Reporting and analytics[5]

Compliance features:

- HIPAA-compliant infrastructure with BAA
- Audit logs for all record access
- Encrypted storage and transmission
- Backup and disaster recovery
- E-signature capabilities
- Retention policy management[4]

Leading Documentation Systems (2026)

SimplePractice

- Comprehensive all-in-one platform
- Telehealth, scheduling, billing, documentation
- Highly customizable intake forms
- Strong client portal features
- Pricing: Tiered based on features ($29-$99/month per clinician) [7]

TherapyNotes

- Robust clinical documentation
- Insurance billing and electronic claims
- Outcome tracking and measurement tools
- Calendar with color-coding and recurring appointments
- Pricing: $59/month per clinician[5]

SimplePractice and TheraNest

- User-friendly interface for solo and group practices
- Note templates, scheduling, billing
- Lower cost option for smaller practices
- Pricing: Starting at $39/month[5]

Cliniko EHR

- Flexible for counseling and multi-disciplinary practices
- Strong treatment planning and progress tracking
- Customizable workflows
- International compliance options[6]

Headway and Alma (for insurance-focused practices)

- Credentialing assistance
- Claims management
- Client matching
- Note: Limited customization compared to full EHR systems[5]

AI-Enhanced Documentation (2026 Update)

Artificial Intelligence is transforming clinical documentation, with tools that generate draft progress notes from session recordings or dictation[8].

Leading AI documentation tools:

Mentalyc

- Therapist-first AI documentation
- Generates clinically sound notes in standard formats (SOAP, DAP, GIRP, BIRP)
- Supports treatment planning and progress tracking across sessions
- HIPAA + BAA, SOC 2 compliant
- Best for: Continuity of care and longitudinal tracking[8]

S10.AI

- 99%+ accuracy with medical-grade precision
- Real-time ICD-10 and CPT coding
- EHR-agnostic compatibility

- HIPAA, GDPR, PIPEDA, ISO 27001 compliant
- Best for: Clinicians requiring audit-ready documentation[8]

Freed AI

- Medical dictation and transcription
- Multi-specialty support
- Voice-to-text with clinical formatting
- Best for: Clinicians preferring dictation workflow[8]

Critical considerations for AI tools:

- Review all AI-generated content before signing
- Ensure clinical accuracy and appropriateness
- Verify BAA coverage for AI processing
- Understand where data is processed and stored
- Maintain professional judgment and clinical reasoning
- Document use of AI assistance per agency/licensing board requirements

---

Telehealth Platforms

Telehealth has become standard practice, requiring secure, reliable platforms that meet both clinical and regulatory standards[9].

Platform Requirements

Essential features:

- HIPAA compliance with signed BAA
- End-to-end encryption
- Waiting room functionality
- Screen sharing capability
- Recording option (with client consent)
- Mobile and desktop compatibility
- Quality audio and video
- Minimal latency and connection issues[9]

HIPAA-Compliant Telehealth Options

Integrated with EHR (recommended):

- SimplePractice Telehealth
- TherapyNotes Video
- Doxy.me (integrates with many EHRs)
- Advantages: Single login, integrated notes, seamless workflow

Standalone platforms:

- Zoom for Healthcare (requires healthcare account with BAA)
- VSee
- Thera-LINK
- Note: Regular Zoom/Skype/FaceTime are NOT HIPAA-compliant[4]

Free HIPAA-compliant options:

- Doxy.me (basic tier with BAA)
- Google Meet (with Google Workspace healthcare account)
- Limitations: Feature restrictions, branding, reliability concerns

Telehealth Best Practices

Technical preparation:

- Test platform before first session
- Use wired internet connection when possible
- Position camera at eye level
- Ensure adequate lighting
- Use headphones for better audio quality
- Have backup communication method (phone)[9]

Clinical considerations:

- Verify client location at start of each session (jurisdiction compliance)
- Confirm private, confidential space for both parties
- Review emergency procedures and local crisis resources
- Document telehealth modality in session notes
- Assess ongoing appropriateness of telehealth for each client[2]

Secure Communication Tools

Communication with clients outside sessions requires HIPAA-compliant solutions[4].

Email

HIPAA-compliant email options:

- Hushmail
- ProtonMail Business
- Paubox
- Your EHR's secure messaging (preferred)

Best practices:

- Use encrypted email for any communication containing PHI
- Never send PHI via regular email
- Include disclaimer in signature about email security limitations
- Obtain client consent for email communication
- Use secure client portal as primary communication method when possible[4]

Text Messaging

HIPAA-compliant options:

- SimplePractice messaging
- OhMD
- Spruce Health
- TigerConnect

Important: Regular SMS/text messaging is NOT HIPAA-compliant. Appointment reminders containing only date/time (no PHI) may use regular SMS with client consent[4].

Client Portals

Most modern EHR systems include secure client portals offering:

- Secure messaging
- Intake form completion

- Appointment scheduling
- Document upload
- Payment processing
- Session notes access (if you choose to share)

Advantage: Keeps all communication within secure, HIPAA-compliant ecosystem[5].

Billing and Payment Processing

Financial transactions involving client information require HIPAA compliance[4].

Payment Processors

HIPAA-compliant processors:

- Stripe (with healthcare configuration and BAA)
- Square for Healthcare
- PayPal Healthcare
- Integrated EHR payment processing (recommended)

Features to prioritize:

- PCI DSS compliance (credit card security standard)
- Automatic payment plans
- Invoice generation
- Superbill creation
- Insurance claim submission
- Payment tracking and reporting[5]

Insurance Billing

Electronic claims submission:

- Speeds reimbursement
- Reduces errors
- Provides tracking and status updates
- Most EHR systems include this functionality

Clearinghouses:

- Office Ally
- Availity
- Change Healthcare
- Intermediaries that format and submit claims to insurance companies[5]

Scheduling and Appointment Management

Efficient scheduling reduces no-shows and improves practice flow[5].

Features to Look For

- Online booking (with or without approval)
- Automated appointment reminders (email, SMS, or both)
- Recurring appointment scheduling
- Color-coded calendars (for multiple clinicians or appointment types)
- Waitlist management
- Cancelation and rescheduling policies
- Integration with Google Calendar or Outlook
- Client self-scheduling through portal[5]

Best Practices

- Send reminders 48 and 24 hours before appointments
- Include clear cancelation policy in reminders
- Use automated reminders to reduce staff time
- Allow clients to confirm appointments via reminder response
- Track no-show patterns in EHR
- Document late cancelations and no-shows in client record[5]

Data Security and Risk Management

Protecting client data requires technical measures, policies, and ongoing vigilance[4].

Device Security

Computer and mobile device protections:

- Strong passwords (minimum 12 characters, mix of types)
- Multi-factor authentication on all accounts
- Automatic screen lock (maximum 5 minutes inactivity)
- Full-disk encryption enabled
- Up-to-date antivirus and anti-malware software
- Regular software and operating system updates
- Separate user accounts for personal and work use
- Remote wipe capability for mobile devices[4]

Physical security:

- Never leave devices unattended in public
- Use privacy screen filters in public spaces
- Lock office when unattended
- Secure backup drives and external storage
- Shred documents containing PHI
- Use locked file cabinets for any paper records[4]

Network Security

- Use secure, password-protected WiFi
- Never access PHI on public WiFi without VPN
- Implement firewall protection
- Use VPN for remote access to office systems
- Separate guest WiFi from practice network
- Regular network security assessments[4]

Backup and Disaster Recovery

3-2-1 backup rule:

- 3 copies of data
- 2 different storage types
- 1 offsite/cloud backup

Implementation:

- Automated daily backups
- Encrypted cloud backup service
- Regular backup testing and restoration drills
- Documented disaster recovery plan
- Alternative practice location identified
- Communication plan for clients during disruption[4]

Data Breach Response Plan

Required elements:

- Immediate containment procedures
- Assessment of breach scope and affected clients
- Notification requirements (clients, OCR, media if 500+ affected)
- Timeline for notifications (60 days maximum)
- Documentation of breach and response
- Post-breach analysis and prevention measures
- Legal consultation protocol[4]

Implementation Checklist

Before Selecting Technology

- ☐ Review AAMFT Code Section 6 requirements
- ☐ Complete HIPAA compliance training
- ☐ Assess practice needs and workflows
- ☐ Determine budget for technology investments
- ☐ Research state licensure board technology requirements
- ☐ Identify must-have vs. nice-to-have features

Vendor Evaluation

- ☐ Verify HIPAA compliance and BAA availability
- ☐ Check security certifications (SOC 2, ISO 27001)
- ☐ Review data encryption methods (in transit and at rest)
- ☐ Confirm data backup procedures
- ☐ Understand data ownership and portability
- ☐ Test platform with free trial or demo
- ☐ Read user reviews from other therapists
- ☐ Verify customer support availability and quality

- ☐ Check integration capabilities with other tools
- ☐ Review contract terms and cancelation policies[4]

Implementation

- ☐ Sign BAA before entering any client data
- ☐ Configure security settings (MFA, auto-logout, etc.)
- ☐ Set up user accounts with role-based permissions
- ☐ Customize templates and forms
- ☐ Import existing client data securely
- ☐ Train all staff on platform use
- ☐ Create written policies and procedures
- ☐ Update informed consent documents
- ☐ Develop technology-specific consent forms
- ☐ Test all workflows before going live[5]

Ongoing Compliance

- ☐ Conduct annual risk assessments
- ☐ Provide annual HIPAA training to all staff
- ☐ Review and update policies annually
- ☐ Monitor vendor compliance and security updates
- ☐ Review audit logs regularly
- ☐ Test backup restoration procedures
- ☐ Update technology as needed to maintain currency
- ☐ Participate in continuing education on technology ethics
- ☐ Document all technology training and competence[2][4]

Common Technology Pitfalls to Avoid

Using non-compliant platforms:

- Regular Zoom, Skype, FaceTime, Google Meet (without healthcare account)
- WhatsApp, Facebook Messenger, regular SMS
- Personal email accounts
- Consumer Dropbox, Google Drive without BAA[4]

Inadequate consent:

- Failing to obtain written consent for technology use
- Not explaining risks and limitations
- Missing emergency procedures in telehealth consent
- No discussion of technology alternatives[2]

Insufficient training:

- Using platforms without proper training
- Not staying current with security updates
- Failing to train staff on HIPAA policies
- Inadequate documentation of competence[2]

Poor security practices:

- Weak passwords or password reuse
- No multi-factor authentication
- Leaving devices unlocked
- Accessing PHI on public WiFi without VPN
- Failing to update software promptly[4]

Documentation gaps:

- Not documenting telehealth modality in notes
- Missing client location for jurisdictional compliance
- Inadequate informed consent documentation
- No written privacy policies for technology[2]

Resources for Ongoing Learning

Professional organizations:

- AAMFT Technology Resources: www.aamft.org
- APA Telepsychology Guidelines
- NASW Technology Standards

HIPAA compliance:

- HHS Office for Civil Rights (OCR): www.hhs.gov/ocr
- HIPAA Journal: www.hipaajournal.com
- Paubox HIPAA Guide: www.paubox.com/blog

Technology reviews:

- Capterra (therapy software reviews)
- Software Advice (EHR comparisons)
- Private Practice Skills Podcast

Security tools:

- Have I Been Pwned (password breach checking): haveibeenpwned.com
- Two Factor Auth List (2FA availability): 2fa.directory
- Privacy Guides: privacyguides.org

Conclusion

Technology integration in therapy practice offers tremendous benefits for efficiency, client care, and practice growth. However, these benefits come with serious ethical and legal responsibilities. By understanding AAMFT Code Section 6 requirements, maintaining HIPAA compliance, selecting appropriate platforms, and implementing strong security practices, therapists can leverage technology while protecting client welfare and maintaining professional integrity.

Key takeaways:

- AAMFT Code Section 6 establishes ethical framework for technology use
- HIPAA compliance is mandatory, not optional
- All vendors handling PHI must sign BAAs
- Informed consent must address technology-specific risks
- Competence requires training and ongoing education
- Security is a continuous process, not a one-time setup
- Regular risk assessments and policy updates are essential

Technology should enhance, not replace, clinical judgment and the therapeutic relationship. When implemented thoughtfully and ethically, technology becomes a powerful tool for delivering quality care while meeting professional standards[2].

References

[1] American Association for Marriage and Family Therapy. (2015). *AAMFT Code of Ethics*. https://www.aamft.org/AAMFT/Legal_Ethics/Code_of_Ethics.aspx

[2] American Association for Marriage and Family Therapy. (2015). AAMFT Code of Ethics: Standard VI - Technology-Assisted Professional Services. https://www.aamft.org/AAMFT/Legal_Ethics/Code_of_Ethics.aspx

[3] HelloNote. (2026, January 28). HIPAA compliance for therapy practices. https://hellonote.com/ensure-therapy-practice-hipaa-compliant/

[4] Paubox. (2025, December 28). Best HIPAA compliant tools for therapy practices. https://www.paubox.com/blog/best-hipaa-compliant-tools-for-therapy-practices

[5] OptiMantra. (2026, February 13). Best therapy practice management software in 2026. https://www.optimantra.com/blog/best-therapy-practice-management-software-in-2026

[6] Clinik EHR. (2026, January 26). Top 5 EHR for counselling 2026: Complete comparison & buyer's guide. https://clinikehr.com/blog/top-5-ehr-counselling-2026

[7] Giva. (2025, April 23). 5 top HIPAA-compliant apps for therapists. https://www.givainc.com/blog/hipaa-compliant-apps-therapists/

[8] Mentalyc. (2026, February 1). AI in clinical documentation 2026: What will matter more than speed. https://www.mentalyc.com/blog/ai-in-clinical-documentation

[9] Two Rivers Therapy Colorado. (2023, December 9). 5 effective techniques for clinical supervision. https://www.tworiverstherapycolorado.com/blog/effective-techniques-for-providing-clinical-supervision