Tali

AI Scribe Privacy and Compliance Checklist

Tali AI's AI Scribe Privacy and Compliance Checklist

At Tali, we aim to help clinicians focus on their patients — not paperwork.

This checklist is designed to help you navigate the implementation of an AI Scribe solution, like Tali, while protecting patient privacy, maintaining security, and meeting regulatory requirements. By following these best practices, you'll not only ease clinical documentation burdens but also build trust among clinicians and patients

Why Privacy and Compliance Matter

Tali AI, we believe in freeing clinicians from administrative tasks so they can focus on patient care. Our commitment includes guiding you through privacy and compliance considerations, ensuring that adopting an AI Scribe is both seamless and secure for everyone involved.

Understand Your Legal and Compliance Context

Before implementing an AI Scribe, it is essential to understand the legal and regulatory landscape governing patient data protection. This ensures that your organization remains compliant and prepared for audits or inquiries.

□ Identify Applicable Privacy Laws

- Determine which regional health privacy legislation (e.g., PHIPA in Ontario) or federal PIPEDA applies to your organization.
- This helps you establish a solid legal foundation from Day One.

□ Clarify Responsibilities

- Map out your team's responsibilities to ensure everyone knows their part to manage compliance.
- Confirm who is accountable for consent, privacy oversight, incident response, and ongoing compliance.

Conduct a Privacy Impact Assessment (PIA) or Risk Assessment

A Privacy Impact Assessment (PIA) or risk assessment helps you proactively identify and mitigate potential privacy and security risks.

□ Visualize Your Data Flow

- Ensure you understand how patient data is collected, processed, and stored. Your AI Scribe vendor should provide relevant information to help you see the big picture.

□ Identify Risks

- Pinpoint potential privacy and security risks (e.g., unauthorized access, re-identification) and develop strategies to mitigate these risks (e.g., encryption, secure access policies). Your AI Scribe vendor should assist in this process.
- Some regions have specific requirements, such as Alberta, Canada, requiring a PIA update. Your AI Scribe vendor should provide templated materials to guide you through this process.

□ Keep a Record of Findings

- Document your assessment for future reference or regulatory inquiries. This demonstrates due diligence and simplifies future updates as technology evolves.

Consent and Patient Communication

Effective communication ensures that patients understand how AI Scribes handle their data and empowers them to make informed decisions.

□ Informed Consent

- Clearly explain to patients why you're using an AI Scribe, how data flows, and how long it is retained. Offer simple ways to give or withdraw consent, whether verbally or in writing. Your AI Scribe vendor should provide materials to support this.

□ Privacy Notices

- Post transparent, easy-to-read information in waiting areas, patient portals, or exam rooms about how the AI Scribe works and patients' rights. Encouraging openness fosters patient trust.

□ Use Vendor Templates

- Create patient-facing material to make patient education quick, clear, and consistent. Your AI Scribe vendor should offer consent forms, infographics, or FAQs that can be adapted to fit your local workflows.

Data Storage, Usage, Retention, and Destruction

Ensuring data security throughout its lifecycle is key to maintaining patient trust and regulatory compliance.

□ Storage Location & Security

- Confirm where data is processed and stored (e.g., Canadian vs. US servers). Check for safeguards like encryption (in transit and at rest) and multifactor authentication.

□ Retention Policies

- Determine how long recordings or transcripts remain on the AI Scribe vendor's servers or in your system.

□ Secure Destruction

- Verify how (and when) the AI Scribe vendor deletes data. Make sure your policy reflects this process for maximum transparency.

□ Vendor Data Practices

- Check if your AI Scribe vendor uses audio/transcripts for AI training or other purposes. Confirm the vendor's approach and request supporting documentation.

Security and Incident Response

Strong security measures help protect patient information from breaches and unauthorized access.

Security Questions to Consider:

What is your development lifecycle?

- This ensures the AI Scribe vendor actively reviews and updates their product for security.

Do you enforce MFA (multifactor authentication)?

- MFA is a simple but powerful security booster.

What is your incident response plan?

- Quick detection and communication minimize potential harm

How do you manage vulnerability upgrades?

- Proactive patching helps prevent breaches

How often do you back up critical data?

- Backups are key to resilience.

What encryption methods do you use (at rest & in transit)?

- Strong encryption safeguards sensitive information.

How do you audit system changes and manage access?

- Comprehensive logging and clear procedures help prevent misuse.

Other Helpful Information to Ask For:

Security Certifications

- Ask if the AI Scribe vendor meets standards like SOC 2, ISO 27001, or HITRUST. Independent certifications signal a robust security posture.

Incident Response

- Work with your AI Scribe vendor to define responsibilities and response times in case of a breach. A shared plan ensures quick, confident action when it matters most.

Contractual and Organizational Readiness

Ensuring clear agreements and internal policies helps streamline AI Scribe implementation.

□ Vendor Contracts

- Make sure your contract with the AI Scribe vendor details each party's roles and obligations.

□ Internal Policies

- Update your privacy and data-handling policies to reflect new AI Scribe workflows. Ensure these updates are visible and accessible to all relevant staff.

□ Staff Training

- Train your staff on the benefits and improvements AI Scribes bring to their workflow. Educate team members on handling AI-generated transcripts and following appropriate access protocols.

Ongoing Governance, Monitoring, and Review

Continual evaluation helps maintain compliance and improve processes over time.

□ Regular Audits

- Plan annual or biannual reviews to confirm continued compliance and adapt to any regulatory changes.

□ Post-Implementation Feedback & Training

- Gather feedback from patients and clinicians to refine your AI Scribe implementation. Conduct regular training sessions on consent best practices, privacy, and technology improvements.

Communication and Transparency

Keeping all stakeholders informed fosters trust and smooth adoption of AI Scribe technology.

□ Patient-Facing Communications

- Maintain an updated FAQ, poster, or online resource describing how the AI Scribe protects privacy and security.

□ Internal Clarity

- Ensure all staff know exactly whom to contact for AI Scribe–related questions or to report any issues.

□ Vendor Collaboration

- Stay in touch with your AI Scribe provider for updates or improvements. Your vendor should provide continuous updates on product improvements or new training materials.

Wrap-Up

By following this Privacy and Compliance Checklist, you can confidently roll out an AI Scribe like Tali while maintaining strong protections for patients' personal health information. Each step helps you not only meet or exceed legislative requirements but also earn the trust of clinicians and patients alike. Embracing new technology can be exciting, and with the right precautions in place, you can enjoy its benefits while safeguarding everyone's privacy. We're here to help every step of the way!

Focus on patients, not paperwork.

Tali

For more information or to book a demo

tali.ai | help@tali.ai

Follow us