CliniScripts

PRIVACY IMPACT ASSESSMENT & THREAT-RISK ASSESSMENT SUMMARY FOR CLINISCRIPTS

By

DELTA DYNAMICS

Date: December 12, 2024

CONFIDENTIAL: This document's contents are privileged and intended solely for the addressee. This transmission is sent in trust, for the sole purpose of delivery to the intended recipient. Do not distribute, email, fax, or transfer to third parties via any mechanism without prior approval of Delta Dynamics. Do not share any of the information contained within this report with third parties unless it is cited from public sources

Acceptance of Privacy Impact and Threat Risk Assessment

Client Acceptance

1. I agree with the TRA scope and the asset classification matrix.
2. I agree with the PIA scope and the sensitivity rating.
3. I acknowledge the listed identified mitigations are currently in place or planned.
4. I agree with the current risk posture and, based on sound business decisions will accept responsibility for implementing the recommendations, implementing alternative safeguards or accepting the risks.
5. I acknowledge the listed identified safeguards are currently in place or planned.
6. I agree with the current risk posture and, based on sound business decisions, will accept responsibility for implementing the recommendations, implementing alternative safeguards or accepting the risks.
7. Finally, I accept all residual risk resulting to the program after the implementation (or non-implementation) of the recommendations.

On behalf of Cliniscripts

Signature:

Mubashir Khan

Chief Privacy Officer

Date: Dec 12, 2024

Acknowledgement by Delta Dynamics

1. I acknowledge that this document is prepared in accordance with HTRA standard procedures and methods for performing Privacy Impact Assessments and Threat-Risk Assessments.
2. I agree with its scope and the asset classification matrix, stated risk posture and recommendations.

On behalf of Delta Dynamics

Signature

Syed Talal Hassan Bukhari, CISA, CISSP, ISO 27001 LA, CAF

Principal GRC Consultant

Date: Dec 12, 2024

Privacy Impact Assessment Summary

1. Product/Service Background

CliniScripts is a SaaS-based automated note-taking application designed for healthcare professionals to streamline capturing and organizing clinical notes from patient interactions. The application leverages advanced technologies like speech-to-text, video-to-text, and image-to-text to transcribe and document medical consultations.

2. PIA Methodology

The methodology used by the Province of Ontario has been applied and adapted to add the additional jurisdictions of the United States and the European Union privacy legislation. Cliniscripts has been assessed according to the ten Fair Information Principles as published by the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information and in accordance with the PIA guidelines issued by the Information and Privacy Commission of Ontario with respect to healthcare.

3. PIA Scope

Scope of the PIA as it relates to the solution being submitted. Focuses on CliniScripts' automated note-taking application and backend integrations.

4. Key Features

1. **Speech-to-Text Conversion:** Real-time transcription during online consultations.
2. **Image-to-Text Conversion:** Converts uploaded images into text.
3. **Audio-to-Text Conversion:** Converts uploaded audio files into text.
4. **Video-to-Text Conversion:** Transcribes spoken words from videos into text.
5. **Vague Conversation:** Blurs mentions sensitive topics like substance abuse in notes.
6. **Cliniko Integration:** Summarizes and sends notes to Cliniko EMR.
7. **Notes Templates:** Customizable templates for common consultations.
8. **Non-Persistent Data Storage:** Data is deleted once the transcription process is complete.

5. Compliance with PIPEDA & PHIPA

1. **Accountability:** Designated roles for privacy compliance.
2. **Identifying Purposes:** Clear communication of data collection purposes.
3. **Consent:** Responsibility lies with healthcare practitioners using the app. Limiting Collection, Use, Disclosure, and Retention: Strict no-data storage policy; data deleted post-consultation.
4. **Safeguards:** Robust security measures and annual audits.
5. **Openness and Individual Access:** Documented policies and procedures.

6. PIA Findings

Category	Control	Risk	Recommendation
Unauthorized Data Access	No data storage: data deleted post-transcription.	**Low**	Annual vulnerability assessment and penetration testing.
Data Breach	Data is not stored; temporary storage only.	**Low**	Annual vulnerability assessment and penetration testing.
Insider Threats	No persistent data storage; access controls in place	**Low**	Semi-annual security awareness training
Inadequate Encryption	Data encrypted via AWS services during processing	**Low**	Annual internal audit to ensure encryption standards
Third-Party Service Vulnerabilities	Usage of secure AWS and OpenAI services; BAA agreements in place	**Low**	Publicly accessible BAA, annual internal audit
Access Control Failures	Least privilege principles; IAM policies	**Low**	Enable multi-factor authentication, quarterly security reviews
Insufficient Data Anonymization	No data storage; real-time processing	**No Risk**	Publicly accessible BAA, annual internal audit
Data Retention and Disposal Issues	Zero data retention policy	**Low**	Publicly accessible BAA, confirmation pop-up for data deletion, annual audit
Unauthorized Data Upload	Images handled by OpenAI with limited retention	**High**	Disable image upload option
Unauthorized PHI Disclosure	Data shared only with authorized services; no persistent storage	**Low**	Publicly accessible BAA, annual internal audit

7. Statement of Responsibility

Delta Dynamics conducted this PIA in accordance with established standards, verifying the accuracy and completeness of the information provided by CliniScripts.

Threat Risk Assessment Summary

1. Purpose and Scope

The report, prepared by Delta Dynamics for Markitech Inc., evaluates the security risks of the Cliniscripts application, a SaaS platform for mental health professionals. The application automates tasks like intake, scheduling, note-taking, and billing, leveraging generative AI for real-time transcription. The TRA assesses risks, safeguards, and provides actionable recommendations to ensure compliance with data protection laws like PIPEDA, PHIPA, and HIPAA.

2. Key Features of Cliniscripts

1. **Automation and Efficiency:**
   - Real-time transcription for patient interactions.
   - Speech-to-text, video-to-text, and AI-supported summarization.
   - Supports integration with EMR/EHR systems.

2. **Market and Value Proposition:**
   - Enables practitioners to see more patients weekly, increasing revenue by $500–$1,200.
   - Designed for mental health practices with privacy compliance as a priority.
   - Offers scalable pricing from small clinics to enterprise setups.

3. **Infrastructure:**
   - Hosted on Google Cloud Platform (GCP) with strict data localization and encryption standards.

Findings

The report highlights the following critical aspects:

- **Data Sensitivity and Classification:**
    - Confidentiality: Rated HIGH for Personal Information (PI) and Personal Health Information (PHI).
    - Integrity: HIGH for ensuring accuracy in PHI.
    - Availability: Rated MEDIUM, as short-term outages are manageable.

- **Identified Threats:**
    - Unauthorized access (Man-in-the-Middle attacks, insider threats).
    - Ransomware or malware affecting database integrity.
    - Service interruptions due to cloud infrastructure failure.

- **Technical and Non-Technical Safeguards:**
    - Role-Based Access Controls (RBAC) for secure system access.
    - Encryption of data at rest.
    - Disaster recovery and regular backups.
    - Security and privacy awareness training.

Key Risks and Recommendations

- **Default Credentials in GCP:**
  - Risk: Attackers exploiting default settings.
  - Recommendation: Replace default credentials and close unnecessary ports.

- **Man-in-the-Middle Attacks:**
  - Risk: Credential theft during client registration.
  - Recommendation: Implement two-factor authentication with time-limited keys.

- **Malware and Ransomware:**
  - Risk: Corruption or encryption of the database.
  - Recommendation: Regular patches, backups, and restrictions on administrative access.

- **Data Exfiltration by Insiders:**
  - Risk: Theft or misuse of sensitive data.
  - Recommendation: Conduct quarterly audits and enforce stricter role-based access.

- **Cloud Platform Failure:**
  - Risk: Service unavailability due to catastrophic events.
  - Recommendation: Test and revise business continuity plans annually.

- **Security Awareness:**
  - Risk: Breaches due to lack of training.
  - Recommendation: Annual training sessions for all employees and onboarding for new hires.

Regulatory and Compliance Highlights

- The system adheres to:
- Canadian: **PIPEDA, PHIPA.**
- U.S.: **HIPAA.**
- No persistent storage of PHI; temporary storage is deleted post-processing.

Projected Risk Post-Recommendation Implementation

After adopting the proposed recommendations, the risks are expected to reduce significantly, achieving an acceptable residual risk level.

Additional Notes

- **Business Goals:** Achieve $10K Monthly Recurring Revenue (MRR) by 2024 and $1M MRR by 2026.
- **Target Market:** Small to mid-sized clinics with a focus on North American therapists.
- **Ethical Concerns:** Addressing biases in generative AI and securing data privacy.