THREAT-RISK ASSESSMENT SUMMARY

FOR CLINISCRIPTS

By

Date: December 12, 2024

Acceptance of Threat Risk Assessment

Client Acceptance

1. I agree with the TRA scope and the asset classification matrix.
2. I acknowledge the listed identified safeguards are currently in place or planned.
3. 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.
4. 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 Technology 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 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

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.