Privacy Impact Assessment Summary for CliniScripts

How to Read: The below numbered sections are titled according to the risk area as evaluated for that description. Each area for assessment is summarized by:

Control: How CliniScripts handles this area of risk
Risk: Rated as Low, Medium or High
Recommendation: The recommended action to manage the associated risk.

Overview
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.

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.

Privacy Impact Assessment (PIA) Scope & Methodology
- **Scope**: Focuses on CliniScripts' automated note-taking application and backend integrations.
- **Assessment Baseline**: Based on PIPEDA and PHIPA standards.
- **Methodology**: Included data collection, analysis, evaluation, threat modeling, and stakeholder interviews.

Identified Privacy Risks & Controls
1. ****Unauthorized Data Access****:
   - **Control**: No data storage; data deleted post-transcription.
   - **Risk**: Low.
   - **Recommendation**: Annual vulnerability assessment and penetration testing.

2. ****Data Breach****:
   - **Control**: Data is not stored; temporary storage only.
   - **Risk**: Low.
   - **Recommendation**: Annual vulnerability assessment and penetration testing.

Privacy Impact Assessment Summary for CliniScripts

3. **Insider Threats**:
   - **Control**: No persistent data storage; access controls in place.
   - **Risk**: Low.
   - **Recommendation**: Semi-annual security awareness training.

4. **Inadequate Encryption**:
   - **Control**: Data encrypted via AWS services during processing.
   - **Risk**: Low.
   - **Recommendation**: Annual internal audit to ensure encryption standards.

5. **Third-Party Service Vulnerabilities**
   - **Control**: Usage of secure AWS and OpenAI services; BAA agreements in place.
   - **Risk**: Low.
   - **Recommendation**: Publicly accessible BAA, annual internal audit.

6. **Access Control Failures**
   - **Control**: Least privilege principles; IAM policies.
   - **Risk**: Low.
   - **Recommendation**: Enable multi-factor authentication, quarterly security reviews.

7. **Insufficient Data Anonymization:**
   - **Control**: No data storage; real-time processing.
   - **Risk**: No risk.
   - **Recommendation**: Publicly accessible BAA, annual internal audit.

8. **Data Retention and Disposal Issues**:
   - **Control**: Zero data retention policy.
   - **Risk**: Low.
   - **Recommendation**: Publicly accessible BAA, confirmation pop-up for data deletion, annual audit.

9. **Unauthorized Data Upload**:
   - **Control**: Images handled by OpenAI with limited retention.
   - **Risk**: High.
   - **Recommendation**: Disable image upload option.

10. **Unauthorized PHI Disclosure**:
   - **Control**: Data shared only with authorized services; no persistent storage.
   - **Risk**: Low.
   - **Recommendation**: Publicly accessible BAA, annual internal audit.

Compliance with PIPEDA & PHIPA
- **Accountability**: Designated roles for privacy compliance.

Privacy Impact Assessment Summary for CliniScripts

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

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

Conclusion
CliniScripts has implemented comprehensive controls to ensure data privacy and security, with low-risk levels for identified threats. Recommendations for ongoing security measures include regular audits, enhanced training, and strict adherence to data privacy laws.

This summary highlights the key aspects of the Privacy Impact Assessment, showcasing CliniScripts' commitment to data privacy and security while addressing potential risks and compliance measures.

For any questions related to this summary, please contact:

Chief Privacy Office
CliniScripts@Markitech.ca