English Version

Data Security Policy
Last Updated: [Date]

1. Introduction
This Data Security Policy outlines the measures that **tsg aesthetic** employs to protect personal data and ensure compliance with the General Data Protection Regulation (GDPR) and relevant Dutch laws. As the sole employee and practitioner, I am responsible for the implementation of these policies.

2. Data Security Objectives
The primary objectives of this Data Security Policy are to:

- Protect personal and sensitive patient data from unauthorized access, alteration, and destruction.
- Ensure confidentiality, integrity, and availability of patient data.
- Maintain compliance with GDPR and other relevant laws.

3. Security Measures
To safeguard data security, the following technical measures are implemented:

3.1. Technical security:

- Data encryption. All data-in-transit between **MedVault** (patient management application) and Google Firebase (data storage) is encrypted using HTTPS and SSL. Data stored on Firebase is encrypted at rest by Google's encryption standards.
- Access controls. Access to patient data is restricted to authorized users only. As a single-practitioner practice, I am the sole practitioner with access to patient data. Authentication is required before accessing any patient data.
- Authentication. Our Firebase authentication requires a unique user ID and password for access, and multi-factor authentication (MFA) is enabled.
- Regular updates. Operating systems and applications are regularly updated to patch vulnerabilities.

3.2. Physical security:
Our clinic restricts physical access to computers and devices that access patient data, ensuring they are stored in a secure location and are password-protected.

4. Procedural Measures
The following procedural measures are in place to ensure data security:

- Confidentiality agreements. If applicable, any third-party service providers will be required to sign confidentiality agreements to protect patient data.
- Data handling procedures. Procedures for collecting, processing, and storing patient data are documented and adhered to strictly.
- Incident response procedures. A data breach response plan is in place, detailing steps to be taken in the event of a data breach (refer to the separate Data Breach Response Plan document).

5. Staff training and awareness
As the sole employee, I undergo regular training on data security best practices and GDPR

compliance to ensure a high level of awareness and preparedness regarding data security measures.

6. Data sharing protocols
Patient data may only be shared with third parties under strict conditions:

- With patient consent. Explicit consent must be obtained from patients before sharing their data with other healthcare providers.
- Legal obligations. Data may be shared if required by law or regulatory bodies.

7. Monitoring and Auditing
Regular monitoring and auditing of data security practices will be conducted to identify potential vulnerabilities and ensure compliance with this policy.

8. Review and Update
This Data Security Policy will be reviewed annually or when significant changes occur, and updates will be made as necessary to reflect best practices and compliance with current laws.

9. Contact Information
For questions regarding this Data Security Policy, please contact:

- Name: Thomas Bodewes
- Company name: tsg aesthetic / MedVault
- Address: Sint Willibrordusstraat 79-4, 1073 VA Amsterdam
- E-mail: info@tsgaesthetic.nl
- Phone: +31652653911

Dutch Version

Beleid voor Gegevensbeveiliging
Laatst bijgewerkt: [Datum]

1. Inleiding
Dit Beleid voor Gegevensbeveiliging beschrijft de maatregelen die **tsg aesthetic** hanteert om persoonlijke gegevens te beschermen en te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en relevante Nederlandse wetten. Als de enige medewerker en praktijkhouder ben ik verantwoordelijk voor de uitvoering van deze beleidsmaatregelen.

2. Doelstellingen van Gegevensbeveiliging
De primaire doelstellingen van dit Beleid voor Gegevensbeveiliging zijn:

- Persoonlijke en gevoelige patiëntgegevens beschermen tegen ongeoorloofde toegang, wijziging en vernietiging.
- Vertrouwelijkheid, integriteit en beschikbaarheid van patiëntgegevens waarborgen.
- Voldoen aan de AVG en andere relevante wetten.

3. Beveiligingsmaatregelen

3.1. Technische maatregelen
Om de gegevensbeveiliging te waarborgen, worden de volgende technische maatregelen getroffen:

- Gegevensversleuteling. Alle gegevens die tussen **MedVault** (applicatie voor patiëntengegevens beheer) Google Firebase (dataopslag) worden verzonden, zijn versleuteld met HTTPS en SSL. Gegevens die in Firebase worden opgeslagen, zijn versleuteld volgens de versleutelingsnormen van Google.
- Toegangsbeheer. Toegang tot patiëntgegevens is beperkt tot bevoegde gebruikers. Als een eenpersoonspraktijk ben ik de enige zorgverlener met toegang tot patiëntgegevens. Authenticatie is vereist voordat er toegang wordt verkregen tot patiëntgegevens.
- Authenticatie. Onze Firebase-authenticatie vereist een unieke gebruikers-ID en wachtwoord voor toegang, en multi-factor authenticatie (MFA) is ingeschakeld.
- Regelmatige updates. Besturingssystemen en applicaties worden regelmatig bijgewerkt om kwetsbaarheden te verhelpen.

b. Fysieke Beveiliging
Onze kliniek beperkt de fysieke toegang tot computers en apparaten die toegang hebben tot patiëntgegevens en zorgt ervoor dat ze op een veilige locatie worden bewaard en met een wachtwoord zijn beveiligd.

4. Procedurele Maatregelen
De volgende procedurele maatregelen zijn getroffen om de gegevensbeveiliging te waarborgen:

- Vertrouwelijkheidsovereenkomsten. Indien van toepassing, moeten derden die diensten verlenen een vertrouwelijkheidsovereenkomst ondertekenen om patiëntgegevens te beschermen.
- Procedures voor gegevensverwerking. Procedures voor het verzamelen, verwerken en opslaan van patiëntgegevens zijn gedocumenteerd en worden strikt nageleefd.
- Incident respons procedures. Een plan voor het reageren op datalekken is in werking, waarin de stappen worden beschreven die moeten worden ondernomen in het geval van een datalek (zie het aparte document over het Datalekresponsplan).

5. Training en Bewustwording
Als enige medewerker volg ik regelmatig training over de beste praktijken voor gegevensbeveiliging en naleving van de AVG om een hoog niveau van bewustzijn en voorbereiding te waarborgen met betrekking tot gegevensbeveiligingsmaatregelen.

6. Gegevensdelingsprotocollen
Patiëntgegevens mogen alleen onder strikte voorwaarden met derden worden gedeeld:

- Met toestemming van de patiënt. Expliciete toestemming moet worden verkregen van patiënten voordat hun gegevens met andere zorgverleners worden gedeeld.
- Wettelijke verplichtingen. Gegevens mogen worden gedeeld indien vereist door de wet of regelgevende instanties.

7. Monitoring en Auditing
Regelmatige monitoring en auditing van gegevensbeveiligingspraktijken worden uitgevoerd om potentiële kwetsbaarheden te identificeren en naleving van dit beleid te waarborgen.

8. Beoordeling en Bijwerking
Dit Beleid voor Gegevensbeveiliging wordt jaarlijks herzien of wanneer zich significante wijzigingen voordoen, en updates worden gedaan indien nodig om de beste praktijken en de naleving van de huidige wetten te weerspiegelen.

9. Contactinformatie
Voor vragen over dit Beleid voor Gegevensbeveiliging kunt u contact opnemen met:

- Naam: Thomas Bodewes
- Bedrijfsnaam: tsg aesthetic / MedVault
- Adres: Sint Willibrordusstraat 79-4, 1073 VA Amsterdam
- E-mail: info@tsgaesthetic.nl

Telefoonnummer: +31652653911