English Version

Data Breach Response Plan
Last Updated: [Date]

1. Introduction
This Data Breach Response Plan outlines the procedures that **tsg aesthetic** will follow in the event of a data breach involving personal data in compliance with the GDPR (General Data Protection Regulation) and AVG (Algemene Verordening Gegevensbescherming). As the sole employee and practitioner, I am responsible for managing and responding to any incidents involving patient data.

2. Definition of a data breach
A data breach refers to any unauthorized access, disclosure, alteration, or destruction of personal data - whether due to a cyberattack, accidental mishandling, or malicious intent - that could potentially compromise the privacy or security of patient information. Types of data breaches include:

- Confidentiality breach. Unauthorized access to patient records or personal data.
- Integrity breach. Unauthorized alteration of patient data.
- Availability breach. Accidental or unlawful loss or deletion of patient data.

3. Identification of a data breach
The following signs may indicate a potential data breach:

- Unauthorized access to patient records.
- Unusual activity on electronic devices or systems.
- Reports from patients regarding unauthorized sharing of their information.
- Physical evidence of theft or loss of data (e.g., lost devices).

4. Roles and responsibilities
Upon identifying a potential data breach, I am responsible for managing the incident, assessing its impact, and reporting it to the relevant authorities.

5. Data breach response procedure

5.1. Detection and reporting:

- In any event of a potential data breach, we must follow the procedure outlined in this plan immediately.
- Documentation of the breach should include details such as the type of data affected, date and time of the breach, and possible cause.

5.2. Containment and mitigation:

- Contain the breach. Implement immediate steps to prevent further data loss or unauthorized access, such as revoking access or isolating affected systems, to secure any physical or electronic records involved.
- Risk assessment. Determine the severity and extent of the data breach, including the type of data affected, volume, and any vulnerability to misuse.
- Mitigation steps. Steps may include resetting passwords, applying patches, or blocking malicious IPs.

5.3. Notification:

- Data Protection Authority. The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) will be notified within 72 hours if the data breach poses a risk to individuals' rights and freedoms.
- Patients. Affected patients will be notified without undue delay if the data breach risks their privacy or personal security.
    - Notification should include information on the nature of the data breach, potential impact, and suggested measures patients should take to protect themselves.

6. Documentation
Maintain a detailed record of the data breach, including:

- The date and time of the data breach.
- A description of the data involved.
- The steps taken to respond to the data breach.
- Any communications made to affected individuals and authorities.

7. Review and improvement
Following the incident, review the circumstances surrounding the data breach and update security measures and policies as necessary to prevent future occurrences. This includes:

- Root cause analysis. A full investigation to determine the root cause of the data breach and prevent future occurrences.
- Response review. After the data breach is contained, a review is conducted to assess the effectiveness of the response plan and make necessary improvements.

8. Training and awareness
As a single-practitioner practice, I will ensure that I remain informed about data protection best practices and any changes in legislation that may affect the management of patient data.

9. Contact information
For any inquiries regarding this Data Breach Response Plan, 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

Datalekresponsplan
Laatst bijgewerkt: [Datum]

1. Inleiding
Dit Datalekresponsplan beschrijft de procedures die **tsg aesthetic** zal volgen in het geval van een datalek waarbij persoonlijke gegevens zijn betrokken in overeenstemming met de GDPR (General Data Protection Regulation) en AVG (Algemene Verordening Gegevensbescherming). Als de eenmanspraktijk ben ik verantwoordelijk voor het beheer en de reactie op incidenten die patiëntgegevens betreffen.

2. Definitie van een datalek
Een datalek verwijst naar elke ongeoorloofde toegang, openbaarmaking, wijziging of vernietiging van persoonlijke gegevens - hetzij door een cyberaanval, onopzettelijk verkeerd omgaan of kwaadwillende bedoelingen - die mogelijk de privacy of veiligheid van patiëntinformatie in gevaar kan brengen. Typen datalekken zijn onder andere:

- Vertrouwelijkheidslek. Ongeautoriseerde toegang tot patiëntendossiers of persoonsgegevens.
- Integriteitslek. Ongeautoriseerde wijziging van patiëntgegevens.
- Beschikbaarheidslek. Onopzettelijk of onrechtmatig verlies of verwijdering van patiëntgegevens.

3. Identificatie van een datalek
De volgende tekenen kunnen wijzen op een potentieel datalek:

- Ongeoorloofde toegang tot patiëntendossiers.
- Ongebruikelijke activiteit op elektronische apparaten of systemen.
- Rapporten van patiënten over ongeoorloofd delen van hun informatie.
- Fysiek bewijs van diefstal of verlies van gegevens (bijv. verloren apparaten).

4. Rollen en verantwoordelijkheden
Bij identificatie van een potentieel datalek ben ik verantwoordelijk voor het beheer van het incident, het beoordelen van de impact en het rapporteren aan de relevante autoriteiten.

5. Procedure voor het reageren op datalekken

5.1. Detectie en melden

- In geval van een potentieel datalek moeten we onmiddellijk de procedure volgen die in dit plan is uiteengezet.
- Documentatie van het lek moet details bevatten zoals het type getroffen gegevens, datum en tijdstip van het lek en mogelijke oorzaak.

5.2. Beheersing en beperking

- Beperk het datalek. Onderneem direct stappen om verder gegevensverlies of ongeautoriseerde toegang te voorkomen, zoals het intrekken van toegang of het isoleren van getroffen systemen, om alle fysieke of elektronische dossiers veilig te stellen.
- Risicoanalyse. Bepaal de ernst en omvang van het lek, inclusief het type gegevens dat is getroffen, de grootte en eventuele kwetsbaarheid voor misbruik.
- Mitigatiemaatregelen. Stappen kunnen het opnieuw instellen van wachtwoorden, het toepassen van patches of het blokkeren van kwaadaardige IP's omvatten.

5.3. Kennisgeving

- Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens zal binnen 72 uur worden geïnformeerd als het datalek een risico vormt voor de rechten en vrijheden van individuen.
- Patiënten. Getroffen patiënten worden zonder onnodige vertraging geïnformeerd als het datalek hun privacy of persoonlijke veiligheid in gevaar brengt.
    - Kennisgeving moet informatie bevatten over de aard van het datalek, de mogelijke impact en voorgestelde maatregelen die patiënten kunnen nemen om zichzelf te beschermen.

6. Documentatie
Houd een gedetailleerd verslag bij van het datalek, inclusief:

- De datum en tijd van het datalek.
- Een beschrijving van de betrokken gegevens.
- De stappen die zijn genomen om op het datalek te reageren.
- Alle communicatie met getroffen individuen en autoriteiten.

7. Beoordeling en verbetering
Na het incident zal de situatie rondom het datalek worden herzien en zullen beveiligingsmaatregelen en -beleid worden bijgewerkt indien nodig om toekomstige voorvallen te voorkomen. Dit omvat:

- Oorzaakanalyse. Een volledig onderzoek om de oorzaak van het datalek te bepalen en toekomstige voorvallen te voorkomen.
- Evaluatie van de respons. Na beheersing van het datalek wordt een evaluatie uitgevoerd om de effectiviteit van het responsplan te beoordelen en verbeteringen door te voeren.

8. Training en bewustwording
Als een eenpersoonspraktijk zorg ik ervoor dat ik op de hoogte blijf van de beste praktijken voor gegevensbescherming en eventuele wijzigingen in de wetgeving die van invloed kunnen zijn op het beheer van patiëntgegevens.

9. Contactinformatie
Voor vragen over dit Datalekresponsplan 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