Stappen bij een incident of datalek in de zorg

1. **Incident identificeren en registreren**
    - Zodra een incident of datalek wordt ontdekt, moet dit direct gemeld en geregistreerd worden in het incidentenregister. Dit kan variëren van ongeautoriseerde toegang tot patiëntgegevens, verlies van dossiers, of een beveiligingsfout in een systeem.
2. **Schade beoordelen**
    - Beoordeel de aard en omvang van het incident. Welke gegevens zijn gelekt? Hoe ernstig is het incident? Betreft het gevoelige gezondheidsinformatie? Zijn er externe partijen bij betrokken?
3. **Beperk de schade**
    - Onderneem direct actie om de impact van het datalek te beperken. Dit kan betekenen dat je toegang tot bepaalde systemen afsluit, betrokken partijen informeert, en zorgt dat verdere schade of toegang wordt voorkomen.
4. **Melden bij de Autoriteit Persoonsgegevens (AP)**
    - Als het datalek aanzienlijke risico's met zich meebrengt voor de privacy van betrokkenen, moet je dit binnen 72 uur melden aan de Autoriteit Persoonsgegevens (AP). Hierbij geef je aan:
        - De aard van het datalek.
        - De gegevens die zijn gelekt.
        - De gevolgen voor de betrokkenen.
        - De genomen maatregelen.
5. **Betrokkenen informeren**
    - Als er een hoog risico bestaat voor de privacy van de betrokkenen (bijvoorbeeld bij het uitlekken van medische dossiers), moet je ook de personen van wie de gegevens zijn gelekt direct informeren. Je moet hen duidelijk uitleggen wat er is gebeurd, welke gegevens zijn getroffen, en welke maatregelen zij kunnen nemen om zich te beschermen.
6. **Oorzaken achterhalen en actie ondernemen**
    - Onderzoek de oorzaak van het incident en neem maatregelen om herhaling te voorkomen. Dit kan betekenen dat je technische beveiligingsmaatregelen aanscherpt, medewerkers beter opleidt, of procedures aanpast.
7. **Evaluatie en rapportage**
    - Zorg ervoor dat het incident gedetailleerd wordt gedocumenteerd. Dit rapport bevat alle relevante informatie

over het incident, de getroffen maatregelen, en de lessen die je hebt geleerd. Dit helpt bij de interne evaluatie en kan van pas komen bij toekomstige audits.

8. **Beleid bijwerken**
    - Werk het beveiligingsbeleid en de procedures bij om te voorkomen dat een dergelijk incident opnieuw plaatsvindt. Zorg dat je organisatie en medewerkers goed op de hoogte zijn van het nieuwe beleid.
9. **Ondersteuning bieden aan getroffen cliënten**
    - Bied eventueel aanvullende ondersteuning aan cliënten van wie de gegevens zijn getroffen, zoals het aanbieden van monitoringdiensten om identiteitsdiefstal te voorkomen.