

1



Een security management op basis van risicoanalyses

We hebben een informatiebeveiligingsplan en doen periodieke controles.
Wij zorgen ervoor dat het ziekenhuis voldoet aan de laatste wet- en regelgeving.

2



Een inventarisatie van alle gegevens, digitale infrastructuur en systemen

Het ziekenhuis heeft procedures ontwikkeld en beschermt data op elk moment.
Wij controleren onze leveranciers en zorgen ervoor dat alle informatie wordt gecommuniceerd.

3



Wij vernietigen de gegevens, indien nodig, veilig en volgens de regels

Het ziekenhuis beschikt over procedures en beschermt data op elk moment.
In geval van twijfel neem contact op met onze Informatie-veiligheidsraadgever.

4



Wij vragen om het bewijs van de vernietiging van vertrouwelijke documenten en media

We werken samen met gespecialiseerde bedrijven op basis van goed gedefinieerde principes.

5



We communiceren en informeren onze patiënten op transparante wijze

We informeren regelmatig onze patiënten over de manier waarop we informatie verwerken.
We vragen toestemmingen en hebben duidelijke procedures.

6



Het ziekenhuis zorgt voor een goede houding tegenover Privacy, smartphones en mobiele apparaten

Wij streven er voortdurend naar om datalekken of externe inbraak te voorkomen.
Wij respecteren het beroepsgeheim en houden onze data veilig.

7



Alle persoonlijke en gevoelige gegevens worden behandeld in overeenstemming met de richtlijnen en wetten.

We hebben een informatiebeveiligingsplan en voeren regelmatig controles uit betreffende de specifieke doeleinden.

8



Security Management geldt zowel voor interne als externe medewerkers

Alle onze partners zijn op de hoogte van onze regels.
In geval van twijfel neem contact op met onze Informatie-veiligheidsraadgever.

9



Het ziekenhuis traint en leidt zijn personeel op.

Wij organiseren bewustmakingscampagnes.
Wij zorgen ervoor dat de verwerking van gegevens en de bescherming van de persoonlijke levenssfeer de onze wordt.

10



Het ziekenhuis heeft een Data Protection Officer aangewezen

Uw DPO waakt over alle aspecten van de bescherming van persoonsgegevens.

11



Wij monitoren en analyseren continu de risico's en indien nodig passen wij onze werkwijze aan

Het risicobeheersplan bevat alle veiligheidsaspecten van het ziekenhuis, met inbegrip van de gegevens van derden waarmee het ziekenhuis samenwerkt.

12



Onze incidentbeheersplan is getest en wordt periodiek geëvalueerd

Het incident-beheersplan, waaronder «datarecovery» en «datacontinuity» wordt automatisch gestart bij vermoedens van inbraak en / of verlies van gegevens.