Spaarne Gasthuis
ACADEMIE

Doe je onderzoek?

Neem informatiebeveiliging serieus!

1. Zet geen persoonsgegevens* in je analysebestand.
2. Duid proefpersonen in al je analysebestanden alleen aan met een niet tot de persoon herleidbare code.
3. Bewaar de sleutel (code verificatielijst) beveiligd met een wachtwoord in een aparte map op de h-, j- of i-schijf van het Spaarne Gasthuis.
4. E-mail geen persoonsgegevens naar een e-mailadres buiten het Spaarne Gasthuis. Zet tot personen herleidbare gegevens dus ook niet op laptops, usb-sticks, externe harde schijven of in 'the cloud'.
5. Een analysebestand ZONDER persoonsgegevens* mag je wel buiten het ziekenhuis bewerken, maar zorg ervoor dat de gegevensdragers (zoals je eigen laptop of i pad) beveiligd zijn met bijvoorbeeld een wachtwoord.
6. Om de juistheid van onderzoeksdata te verifiëren, mag je de persoonsgegevens wel delen met de behandelaars van de patiënt.
7. Bekendmaking van persoonsgegevens aan derden kan alleen op basis van wettelijk voorschrift (bijvoorbeeld IGZ, erkende METC).
8. Persoonsgegevens mogen worden gedeeld bij een calamiteit in het onderzoek of indien nodig voor interne controle van de onderzoeksresultaten (bijvoorbeeld aan raad van bestuur, monitor van het wetenschapsbureau, METC of ACLU).
9. Studiemonitors en onderzoekers mogen alleen toegang tot de, voor de studie ingerichte, studie-inbaskets waarin de dossiers van de proefpersonen door de onderzoeker zijn geplaatst. Een monitoraccount is verkrijgbaar bij het wetenschapsbureau.
10. Houd je aan de 10 gouden regels over informatiebeveiliging. Mocht het toch mis gaan, meld een datalek dan bij de functionaris gegevensbescherming.

* Onder persoonsgegevens verstaan we herleidbare gegevens naar de persoon, waaronder naam, patiëntennummer, adresgegevens, BSN-nummer, e-mailadres.