4 BEVEILIGING

- Alle medewerkers van het KinderKennisCentrum zijn verantwoordelijk voor alle aspecten van beveiliging binnen de eigen invloedssfeer, zoals deur op slot aan het einde van de dag, computer vergrendelen bij het verlaten van de kamer, laptops aan een kabel, apparatuur niet laten slingeren of achterlaten in de auto, clean desk, 'dwalende' en/of onbekende personen aanspreken.

- Bij verwijdering of hergebruik van apparatuur met informatiedragers (o.a. harde schijven maar ook bijv. geheugenkaartjes van camera's) wordt de daarop aanwezige informatie vernietigd of overschreven.

- De medewerkers van het KinderKennisCentrum maken gebruik van persoonlijke inlogaccounts. Accounts worden niet gedeeld. Dan is al snel niet meer duidelijk wie gebruik maakt van het account en kan het wachtwoord niet meer gewijzigd worden.

- Indien een beveiligingsincident wordt geconstateerd (bijv. ongeautoriseerde toegang tot de data of diefstal van data), dient direct contact opgenomen te worden met het Computer Emergency Response Team UU (CERT-UU) en de Datamanager. Het team is 7 dagen per week bereikbaar voor calamiteiten.

YOUth

Onderzoek naar de ontwikkeling van kinderen in de regio Utrecht

GEDRAGSCODE VOOR BEHEER EN GEBRUIK DATA

CONTACTGEGEVENS

Computer Emergency Response Team UU
Vermoed je misbruik of inbreuk op de beveiliging? Neem dan zo snel mogelijk contact op met het Computer Emergency Response Team (CERT-UU).
CERT-UU is maandag t/m zondag bereikbaar van bereikbaar van 8.30 – 23.00 uur.
E-mail: cert-uu@uu.nl, telefoon: +31 (30) 253 5959 (voor spoedeisende gevallen).

Datamanager KinderKennisCentrum:
Voor alle vragen rondom data kun je contact opnemen met de datamanager van het KinderKennisCentrum:
Malu Parson, e-mail: kinderkenniscentrum@uu.nl of m.parson@uu.nl

Voor meer informatie zie ook het datamanagementplan.

Medewerkers van het KinderKennisCentrum werken dagelijks met onderzoeksdata die van groot belang zijn voor de maatschappij waarin wij leven en de instellingen waar wij voor werken. De maatschappij investeert in het YOUth onderzoek door middel van financiering en participatie. Zij mogen van ons verwachten dat wij daar zorgvuldig mee omgaan en ons inzetten voor transparantie, duurzaamheid en integriteit van onderzoek. Om die reden zijn alle relevante wetten en regels voor YOUth geconcretiseerd naar onderstaande richtlijnen. De richtlijnen zijn verdeeld naar vier onderwerpen:

1. OPSLAG | 2. DELEN | 3. PRIVACY | 4. BEVEILIGING

1. OPSLAG

- De onderzoeksdata zijn veilig door ze op Yoda (de Y-schijf) te zetten en te houden. Dit geldt voor alle data: ruwe data, bewerkte data, syntaxen, et cetera. Dit zorgt voor:
  - De beveiliging tegen verlies en aantasting: Yoda slaat data op meerdere locaties op.
  - De beveiliging tegen ongeautoriseerde toegang.
  - De vindbaarheid van data, doordat op Yoda automatisch metadata worden toegevoegd.
  - De beschikbaarheid van data: Yoda is als centrale voorziening bij een professionele beheerorganisatie in beheer.
  - De herleidbaarheid van data: Yoda plaatst automatisch ruwe brondata in een kluis.
  - De duurzame opslag, doordat de onderliggende opslagsystemen tussentijds gemoderniseerd worden.
  - Gecontroleerde en onherroepelijke vernietiging, doordat data op gestructureerd wijze is opgeslagen en tevens bekend is wie de data heeft verkregen.

- MRI beelden worden opgeslagen bij het UMCU evenals de (meta) data van biologisch materiaal.

- Medewerkers van het KinderKennisCentrum laten onderzoeksdata niet rondzwerven. Onderzoeksdata worden niet mee naar huis genomen en niet op (onbeveiligde) USB-sticks gezet. De data op apparatuur van de instelling waar voor gewerkt wordt, is apparatuur die adequaat beveiligd is.

- Om toekomstig gebruik van de data mogelijk te houden, wordend standaard dataformaten gebruikt. Samen met de datamanager kan onderzocht worden wat het meest bestendige dataformaat is.

- Middels versiebeheer is van alle versies duidelijk:
  - Of het ruw 'raw', in bewerking 'intermediate' of definitief 'final' is.
  - Wat de versiedatum is.

- Data ten behoeve van een publicatie wordt nog minimaal 10 jaar na een publicatie bewaard. Alle ruwe data worden minimaal 15 jaar na het verzamelen bewaard, inclusief metadata. Met uitzondering van de direct en indirect identificerende persoonsgegevens. Deze worden slechts, zolang redelijkerwijs voorzienbaar dat zij voor het desbetreffende onderzoek kunnen worden gebruikt, opgeslagen.

2. DELEN VAN DATA

- De verzamelde gegevens worden uitsluitend voor onderzoeksdoeleinden gebruikt en niet voor bijvoorbeeld screenen van deelnemers op (erfelijke) ziektes.

- Indien medewerkers of externen de data eerder willen verkrijgen, kunnen zij een verzoek indienen bij de Data Management Commissie. Deze toetst onder andere het doel van de aanvraag met het informed consent en beslist of de data beschikbaar worden gesteld. Voor medewerkers die helpen met het verzamelen of de kwaliteit toetsen van de data geldt een uitzondering; voor deze werkzaamheden is geen toestemming vereist evenals t.a.v. de pilot data. Voor analyses t.a.v. onderzoek uiteraard wel.

3. PRIVACY

- De medewerkers van het KinderKennisCentrum werken met gepseudonimiseerde data. Dit geeft de hoogste bescherming van de persoonlijke levenssfeer van de deelnemers binnen de gestelde kaders van het onderzoek.

- Alle medewerkers van het KinderKennisCentrum zijn individueel verantwoordelijk voor het handhaven van het informed consent en het beschermen van de privacy van de deelnemer. Zo worden er geen direct of indirect herleidbare persoonsge gevens geregistreerd. Ook niet in onze aantekeningen.

- De medewerkers van het KinderKennisCentrum verrichten geen handelingen met bestanden van anonieme gegevens (koppelingen, vergelijkingen, bewerkingen), waarmee de identiteit van deelnemers kan worden herleid.

- Direct herleidbare persoonsgegevens zijn in ieder geval: (voor-)naam(en), voorletters, titulatuur, geslacht, geboortedatum, e-mail adres, woonadres, telefoonnummer, burger servicenummer en bank- en gironummer.

- Indirect herleidbare persoonsgegevens zijn gegevens waarmee de identiteit van de persoon alsnog achterhaald kan worden. Bijvoorbeeld het beroep dat iemand uitoefent. Indien er maar weinig personen zijn in deze groep, is de persoon makkelijk te herleiden. Te denken valt bijvoorbeeld aan Minister President of de combinatie van de functie schooldirecteur en postcode.