Bijlage 7

Gedragsregels t.a.v. privacygevoelige informatie

1. UZI-passen

- De UZI-pas bevat een persoonlijke identiteit en een elektronische handtekening van de pashouder. De UZI-pas is daarmee persoonsgebonden en dient alleen door de rechtmatige pashouder gebruikt en niet uitgeleend te worden!
- De pashouder is verantwoordelijk voor het veilig bewaren van de UZI-pas en bijbehorende pincode. De UZI-pas en de pincode mogen in verband met eventueel misbruik niet gezamenlijk worden opgeborgen.
- De pashouder is verplicht om de UZI-pas mee te nemen en te gebruiken tijdens de dienst op de organisatie.
- De pashouder mag de UZI-pas tijdens de dienst niet onbeheerd in de kaartlezer laten zitten.
- De pashouder neemt aan het einde van de dienst de pas uit de kaartlezer en bergt de UZI-pas zorgvuldig op.

2. Papier

- Patiëntgegevens op papier mogen het pand van de CHN niet verlaten, tenzij voor het rijden van een visite.
- ANW: bij het uitprinten van gegevens moeten de documenten direct van de printer worden gehaald.
- Kantoor: bij het uitprinten van privacygevoelige informatie moeten de documenten direct van de printer worden gehaald (in de toekomst kan dit met een wachtwoord).
- Patiëntencontacten mogen niet op bureaus blijven liggen. Informatie moet aan het eind van de dienst op worden geruimd.
- Patiëntencontacten mogen niet onbeheerd in de visiteauto blijven liggen.
- Patiëntencontacten die niet meer nodig zijn, moeten vernietigd worden of in de bak ‘vertrouwelijk papier’ worden gedeponeerd. Deze bak wordt tijdens de dienst meerdere malen versnipperd.

3. E-mail

- Het is niet toegestaan per mail tot de persoon herleidbare patiëntinformatie te versturen, ook niet binnen de organisatie.

4. USB-sticks

- USB-sticks kunnen besmet zijn met virussen of hacker-mogelijkheden. Alleen een USB-stick gebruiken als duidelijk is waar deze vandaan komt, bij voorkeur een beveiligde USB-stick met wachtwoord.
- USB-sticks met patiënteninformatie of organisatiegevoelige informatie mogen niet mee naar huis worden genomen.
- USB-sticks mogen niet in de auto blijven liggen, of ergens anders achtergelaten worden.
- Voor het gebruik van documenten thuis (thuiswerken) kan gebruik gemaakt worden van een beveiligde mailaccount van de organisatie.
- USB-sticks of CD’s met geluidsopnamen blijven altijd op de organisatie en verlaten het pand niet.

5. Thuiswerken

- De CHN biedt geen mogelijkheid tot thuiswerken. Wel kan thuis toegang verkregen

worden tot de persoonlijke mailaccount via de website van het Radboud.
- Locatiemanagers Wijchen en Boxmeer kunnen via een speciale beveiligde verbinding ook op afstand werken.

6. Werken met een laptop
- In de toekomst wordt het werken met een laptop op afstand mogelijk. Hiervoor zullen tezijnertijd diverse veiligheidsmaatregelen worden genomen.
- Bij werken met een laptop op kantoor, laat de laptop ‘s avonds achter in een gesloten kast.

7. Clear desk, clear screen
- Ruim na een werkdag op kantoor je bureau helemaal op. Veel ruimtes worden na kantooruren gebruikt voor ANW-zorg of andere activiteiten (vergaderingen).
- Sluit kasten en ladeblokken af.
- Kantoor: bij afwezigheid (indien mogelijk) je scherm blokkeren.
- In ANW-zorg: zorg dat patiënten geen zicht hebben op gevoelige informatie, bijvoorbeeld aan de balie, maar ook in de spreekkamers. Dit kan door scherm blokkeren dan wel het minimaliseren van privacygevoelige schermen.