

Gedragsregels privacy- en informatieveiligheid

Door de vele technologische ontwikkelingen zal R.K. Zorgcentrum Roomburgh (verder Roomburgh) ook in toenemende mate mogelijk geconfronteerd kunnen worden met pogingen van criminelen om in te breken in de systemen of pogingen op een andere wijze gevoelige informatie van Roomburgh te verkrijgen. Vanuit diverse wetten is Roomburgh verplicht om persoonsgegevens goed te beveiligen maar ook andere informatie moet goed beschermd worden en vertrouwelijk blijven. Daarom verbetert Roomburgh doorlopend de processen en technologie om alle data en bestanden goed te beveiligen.

De Security Officer zorgt er dagelijks voor dat onze ICT infrastructuur optimaal beveiligd is. Maar het belangrijkste uitgangspunt voor informatiebeveiliging dat zijn de medewerkers van Roomburgh zelf. Dit betekent dat elke medewerker in elke situatie in eerste instantie zelf, uitgaande van zijn professionaliteit, een optimale balans vindt in bijvoorbeeld het inzien van of beschikbaar hebben en delen van informatie ten behoeve van een goede dienstverlening **versus** het afschermen van informatie ten behoeve van de vertrouwelijkheid en privacy. Bij Roomburgh gelden de volgende gedragsregels die moeten helpen de (persoons-) gegevens van de cliënten en medewerkers optimaal te beschermen.

Dagelijkse routine

- Een wachtwoord op je laptop/computer/tablet is verplicht. Houd het wachtwoord van je laptop/computer/tablet geheim.
- Werk nooit in elkaars user account.
- Berg vertrouwelijke informatie op in afgesloten kasten en laden. Ruim je bureau op waar het vertrouwelijke gegevens betreft (clean desk) .
- Log uit of vergrendel je laptop/pc als je je werkplek verlaat (clean screen).
- Zet je laptop/PC uit aan het eind van de werkdag.

Printen, versturen, weggooien en vinden

- Adresseer vertrouwelijke informatie altijd aan een persoon – bij voorkeur **niet** aan een groep medewerkers/collega's
- Kies de juiste printer nabij de eigen werkplek (bijvoorbeeld op de zusterpost).
- Roomburgh heeft "beveiligd printen" geïnstalleerd. Dat betekent dat jouw printopdracht alleen uit de printer rolt wanneer je op de printer jouw toegangscode ingeeft. Zo blijven er nooit meer (vertrouwelijke) printjes op de printer liggen. Vraag via je leidinggevende bij de Security Officer je toegangscode aan.
- Gooi vertrouwelijke gegevens na gebruik weg in een afgesloten 'papierbak' (blauwe bak in de gang benden) of papierversnipperaar.
- Alle e-mails waarin persoonsgegevens zijn opgenomen die via je Roomburgh account verstuurt aan een externe ontvanger moeten altijd via Zorgmail worden verstuurd. Mocht je vragen hebben over het gebruik van Zorgmail, wend je dan tot de Security Officer.
- Ruim iedere maand je digitale werkplek op; zorg dat je mailbox en downloadmap / bureaublad iedere vier weken geleegd wordt waarbij informatie die je niet meer nodig hebt of die reeds is opgeslagen verwijderd wordt.

Gebruik van internet, social media, e-mail, telefoon en voicemail

- Wees voorzichtig met het binnenhalen van bestanden van internet, met name .exe bestanden.
- Bezoek geen sites die een verhoogd risico op malware-infectie met zich meebrengen (zoals spelletjes e.d.)
- Geef nooit je Roomburgh inlogcode en wachtwoord op als toegang voor een externe toepassing op internet.
- Wees voorzichtig met wat je plaatst op social media. Noem nooit de naam van een collega of een bewoner/cliënt en zorg ervoor dat ook indirect zijn/haar identiteit niet herleidbaar is. Ga voorzichtig om met de privacy van collega's en cliënten en denk aan de goede naam van Roomburgh.
- Open geen bijlage in verdachte mail. Verdacht is: onbekende afzender (onduidelijk/vreemd emailadres), vreemde teksten (zoals taal- /spelfouten). Reageer niet maar verwijder deze mail.
- De e-mails vanuit jouw Roomburgh-account zijn altijd versleuteld (en dus beveiligd) als je naar een e-mailadres van Roomburgh mailt. Gebruik nooit een privé emailadres om zakelijke mails te versturen. Spreek van tevoren af via welk e-mail adres je je tot de cliënt richt en vanuit welk adres hij/zij jou mailt. Houd je daaraan; gebruik dus niet 'reply' als de cliënt informatie vanaf een ander e-mail adres stuurt, bijvoorbeeld vanuit een onbekend privé e-mailadres. Voorkeur heeft het gebruik van Carenzorg.
- Mail, agenda en contacten kunnen worden gesynchroniseerd naar smartphone of tablet. Beveilig ook deze altijd met een wachtwoord. Verlies je je smartphone of tablet, dan is het risico groot dat de gegevens in je mail (inclusief bijlagen), agenda en contacten 'op straat kunnen komen te liggen'. **Meld het verlies** van smartphone, tablet of laptop altijd **direct** aan de Privacy Officer en de Security Officer. In nood kunnen op afstand alle zakelijke gegevens op jouw smartphone en ipad geblokkeerd / gewist worden.
De Security Officer kan op afstand de synchronisatie van het zakelijke account op een mobiel toestel of ipad op verschillende manieren stopzetten, dit kan door de synchronisatie te stoppen, het apparaat te wissen/verwijderen en door het wachtwoord aan te passen.
- Gebruik geen Whatsapp voor contact met cliënten of tussen collega's onderling over cliënten. Facebook (eigenaar Whatsapp) gebruikt data (of gedragsgegevens) om profielen aan te maken van deelnemers aan de chat en kan (en mag) deze gegevens verkopen aan derden. Gebruik hiervoor privacyvriendelijke alternatieven. Communicatie over cliënten kan bijvoorbeeld via ONS.
- Let op dat bij het maken van foto's van een wond het gezicht van cliënt nooit in beeld is. De cliënt mag onder geen beding herkenbaar in beeld zijn. Verwijder de foto na het uploaden in ONS altijd direct uit de fotobibliotheek van je telefoon / laptop.

Inzage en informatieverstrekking

- Geef nooit cliëntinformatie aan iemand die niet rechtstreeks betrokken is bij de zakelijke relatie.
- Bedenk dat de persoonsgegevens van een contactpersoon bij een cliënt, ook privacygevoelige informatie is.
- Bedenk dat je zelf ook alleen kennis mag nemen van informatie over de cliënt als je rechtstreeks betrokken bent bij de behandeling van de cliënt en voor zover noodzakelijk om je werk goed te doen. Het feit dat je informatie kunt zien, betekent niet dat je deze informatie ook *mag* zien.

- Wees zuinig met het geven van informatie aan derden, beperk je tot het noodzakelijke. Een teveel aan informatie kan oneigenlijk worden gebruikt.
- Informeer een nieuwe cliënt over hoe er bij Roomburgh met persoonsgegevens wordt omgegaan, wie er inzage heeft.

Omgang met vertrouwelijke gegevens

- Neem in principe geen vertrouwelijke gegevens mee naar buiten. Als het echt moet om je werk te kunnen doen, moeten de gegevens versleuteld zijn en van buitenaf niet herkenbaar zijn als vertrouwelijke gegevens. Vertrouwelijke gegevens zijn individuele cliëntgegevens, medewerkersgegevens en bedrijfsgevoelige gegevens. Bij gebruik van vertrouwelijke gegevens buiten kantoor ben je als medewerker steeds verantwoordelijk dat deze gegevens vertrouwelijk blijven. Laptops, smartphones en tablets buiten kantoor nooit onbeheerd achterlaten, bijvoorbeeld in de auto. Verlies van laptop, smartphone, tablet altijd direct melden bij de Privacy verantwoordelijke binnen Roomburgh (Privacy Officer en / of de Security Officer).
- Zorg ervoor dat je geen vertrouwelijke gegevens en bestanden lokaal opslaat. Onze applicaties/cliëntsystemen zijn de plek om alles op te slaan en voldoen aan de benodigde beveiligingseisen.
- Print bij voorkeur geen vertrouwelijke gegevens en bestanden.

TIPS

- Laat geen papieren lijsten met cliëntgegevens / medewerkersgegevens zoals 06 nummers circuleren.
- Als je regelmatig presentaties geeft met behulp van power point / Keynote zet dan vooraf je outlook uit! Anders 'poppen' er tijdens de presentatie regelmatig namen op (vanuit de herinneringswaarschuwing of mail) en zijn er in één klap veel meer mensen op de hoogte met welke cliënten jij werkt dan wenselijk is!
- Maak gebruik van een wachtwoordmanager. Informatie hierover kun je opvragen bij de Security Officer.

Signaleer zelf!

- Signaleer je dat informatie onvoldoende beschermd is of dat er sprake is van een datalek (bijvoorbeeld gegevens blijven liggen in de printer op de gang of je vindt een cliëntrapport op de tafel in de keuken), bespreek dit dan met je betreffende collega.

Roomburgh Wachtwoordbeleid

- Roomburgh werkt met verschillende applicaties die vertrouwelijke gegevens opslaan, daarom stellen we de volgende eisen bij het aanmaken van een wachtwoord:
 - Het wachtwoord moet minstens acht tekens lang zijn;

- Het wachtwoord moet minstens één hoofdletter bevatten;
 - Het wachtwoord moet minstens één kleine letter bevatten;
 - Het wachtwoord moet minstens één cijfer bevatten;
 - Het wachtwoord moet minstens één vreemde teken bevatten.
- Iedere 3 maanden zal je het wachtwoord moeten wijzigen naar een nieuw wachtwoord dat voldoet aan genoemde punten.
- Inloggegevens worden nooit ergens opgeschreven/opgeslagen.
- Een wachtwoord wordt voor één applicatie gebruikt. Eenzelfde wachtwoord voor verschillende applicaties is dus niet toegestaan.
- Wachtwoorden die gebruikt worden voor Roomburgh systemen/applicaties, mogen niet in de privésferen worden gebruikt of andersom.