Ziekenhuis Gelderse Vallei

For your eyes only

Informatiebeveiliging in Ziekenhuis Gelderse Vallei

For your eyes only

Hoeveel mensen weten jouw wachtwoord? Is het bijvoorbeeld 12345? Of de naam van je huisdier of kind? Misschien hangt het wel met een geeltje aan je beeldscherm… Zorgvuldig omgaan met jouw inloggegevens in ons ziekenhuissysteem is belangrijk. Niet alleen voor jezelf, maar vooral voor de beveiliging van de gegevens van onze patiënten. Het gaat onder andere om voor de hand liggende zaken, bijvoorbeeld de samenstelling en het gebruik van je wachtwoord. Een wachtwoord is net als je pincode uniek en 'for your eyes only'. — Dik van Starkenburg, Raad van Bestuur

Informatie... wat is het waard?

Goede informatie is belangrijk voor ieders werk. Niemand kan zonder de juiste informatie op het juiste moment. Verkeerde informatie of het ontbreken van gegevens is in de zorg zelfs levensbedreigend. De informatie waarmee wij werken is bovendien heel gevoelig. Denk aan informatie over de gezondheid van onze patiënten of aan informatie over jouw eigen salaris of werkprestaties. Deze informatie is vertrouwelijk en moet binnen Ziekenhuis Gelderse Vallei dan ook veilig zijn!

Fouten worden duur betaald

Het omgaan met informatie, zowel mondeling als op papier of digitaal, brengt allerlei risico's met zich mee. Onzorgvuldig gedrag leidt tot verlies en in ernstige gevallen misbruik van informatie. Deze fouten worden duur betaald! Niet alleen komt onze goede naam onder druk te staan. Erger is de persoonlijke schade die kan ontstaan, uiteenlopend van blijvend lichamelijk letsel door een verwijtbare medische fout, tot emotionele schade door (al dan niet opzettelijke) schending van de privacy.

Jij bepaalt het succes!

Wij willen dan ook de kwaliteit van onze informatie bewaken en verlies en misbruik voorkomen. Niet alle risico's zijn echter af te dekken met ICT-middelen, een goed slot op de deur en een ondertekende geheim-houdingsverklaring van onze medewerkers. Beveiliging van waardevolle informatie waarmee gewerkt wordt, is mensenwerk. Het vraagt om continue alertheid en bewust gedrag van iedere medewerker.

Wat kan jij doen?

Waar mensen werken, worden fouten gemaakt. Omdat we in semi-openbare gebouwen werken, zijn we nog eens extra kwetsbaar.

Om de risico's zo klein mogelijk te maken, hebben we een aantal afspraken gemaakt. Neem deze ter harte en maak ze onderdeel van jouw dagelijkse routine!

Hieronder staan de afspraken in het kort genoemd. Op ons intranet (de pagina Informatiebeveiliging) vind je tips en de actuele regelingen die voor ons van toepassing zijn en waar je je aan moet houden.

1.Wees zorgvuldig met informatie

- Bescherm de privacy van patiënten en collega's.
- Raadpleeg alleen patiëntengegevens van patiënten waarmee je een behandelrelatie hebt of die nodig zijn voor de uitoefening van jouw functie.
- Deel informatie alleen met degenen die hiertoe bevoegd zijn.
- Laat vertrouwelijke informatie nooit onbeheerd achter.
- Bij gebruik van printers of fax: haal jouw documenten direct op.
- Berg vertrouwelijke papieren of computermedia op in een afgesloten kast of ruimte.
- Bewaar vertrouwelijke gegevens niet langer dan nodig of wettelijk toegestaan.

2.Voorkom dat anderen bij jouw werkplek of PC kunnen

- Draag je personeelspas goed zichtbaar, links op revershoogte.
- Gebruikersnaam en wachtwoord zijn persoonlijk; leen deze nooit uit.
- Groepsaccounts zijn niet toegestaan tenzij de manager I&A een uitzondering maakt.
- Kies een veilig wachtwoord: (hoofd)letters, cijfers en/of speciale symbolen. Wijzig het elk half jaar.
- Vergrendel je PC als je je werkplek verlaat (slotje linksonder op je beeldscherm of Ctrl/alt/del) en/of doe de deur op slot.
- Berg sleutels goed op.
- Ga zorgvuldig om met laptops en USB-sticks en andere mobiele informatiedragers.
- Gebruik alleen software die ZGV beschikbaar stelt.
- Wees zorgvuldig met gegevens op draagbare media zoals USB-sticks of tablets, zeker als deze van onbekende afkomst zijn.

3.Gebruik internet en email verstandig

- Via veel sites wordt ongewenste software stiekem op je pc gezet, beperk je internetgebruik daarom tot het hoogst noodzakelijke.
- Open geen bestanden van onbekende afkomst.
- Wees alert op binnenkomende emails, dit kunnen phishing mailtjes zijn met kwaadaardige bedoelingen.

4.Wees continu alert en bewust

- Meld incidenten en onveilige situaties rond informatiebeveiliging in ons VIM systeem.
- Wees je bewust van het feit dat bijgehouden wordt wie welke informatie opvraagt en dat dit steekproefsgewijs wordt gecontroleerd. Help

collega’s door ze te attenderen op onveilig gedrag.
- Draag suggesties aan bij je leidinggevende om verlies of misbruik van informatie te voorkomen.

Onze regels rond informatiebeveiliging (zie ons intranet voor de meest actuele regelingen) gelden voor alle collega's. Spreek een collega eropaan als deze zich niet aan bovengenoemde maatregelen houdt.

Bij het niet naleven van bovenstaande maatregelen en/of richtlijnen, zoals opgenomen in het beleid voor controle op inzage gegevens, geldt de wegwijzer ‘ongewenst gedrag en disfunctioneren’.