



**MAASSTAD
ZIEKENHUIS**
een santeon ziekenhuis



Gedragsregels

Hoe gaan we om met informatie over patiënten en medewerkers, en met eigendommen van het Maasstad Ziekenhuis.

De gegevens die je in het Maasstad Ziekenhuis gebruikt en verwerkt zijn gevoelig en zeer vertrouwelijk. We hebben het niet alleen over informatie van patiënten, maar bijvoorbeeld ook over persoonsgegevens, salarissen en werkprestaties van medewerkers. Het is belangrijk dat je hier zorgvuldig en bewust mee omgaat.

In deze folder staan de belangrijkste gedragsregels voor het correct omgaan met gevoelige, vertrouwelijke informatie en eigendommen van het Maasstad Ziekenhuis. Voor de beste patiëntveiligheid en onze zorgkwaliteit. Medewerkers, bezoekers, leveranciers en andere 'klanten' van het ziekenhuis

kunnen rekenen op ons zorgvuldig gedrag. Neem de regels daarom aandachtig door en maak ze onderdeel van je dagelijkse routine. Zo houden we samen: "Het Maasstad Ziekenhuis bewust veilig!"

Informatie veiligstellen

We moeten samen voorkomen dat informatie onbedoeld in verkeerde handen valt en vertrouwelijke gegevens worden misbruikt. Dit kan ernstige financiële, psychische en lichamelijke gevolgen hebben voor patiënten, medewerkers en het ziekenhuis. Dit betekent dat je informatie over patiënten en medewerkers veilig moet opslaan, bewaren en afsluiten.



Vergrendel je beeldscherm en laat bedrijfseigendommen nooit onbeheerd achter.

Wees scherp en alert

Voor je het weet gooi je per ongeluk vertrouwelijke informatie in de openbare prullenmand in plaats van in de daarvoor bestemde, afgesloten papiercontainer, haal je onbewust een virus binnen op je computer of trap je in een Phishing mail. Het is zo gebeurd en het zijn risico's waar je bewust van moet zijn.

Het Maasstad Ziekenhuis hecht veel waarde aan het veilig omgaan met (vertrouwelijke) informatie en eigendommen van het ziekenhuis. Wees daarom altijd scherp en alert, ook in situaties die onschuldig lijken. Alleen zo kun je incidenten en eventuele schadelijke gevolgen voor patiënten, medewerkers en het Maasstad Ziekenhuis voorkomen.

De gedragsregels onder elkaar

GEDRAGSREGEL 1

Ga zorgvuldig om met gevoelige informatie.

GEDRAGSREGEL 2

Verwerk en gebruik bedrijfs- en persoonsgegevens op de juiste manier.

GEDRAGSREGEL 3

Gebruik ICT-middelen zorgvuldig.

GEDRAGSREGEL 4

Ga bewust om met internet, e-mail en social media.

GEDRAGSREGEL 5

Voorkom ongeautoriseerde toegang tot je werkplek.

GEDRAGSREGEL 6

Wees continu alert op onveilige situaties.

GEDRAGSREGEL 7

Volg de instructies voor het correcte gebruik van informatiesystemen.

GEDRAGSREGEL 8

Meld incidenten.

Ga zorgvuldig om met gevoelige informatie

- Hoe overtuigend, enthousiast of ontdaan mensen misschien ook zijn, geef geen vertrouwelijke informatie aan onbekenden. Deel informatie alleen met bevoegde personen. Geef ook niet zomaar informatie aan politie, justitie of andere overheidsinstanties. Raadpleeg bij twijfel altijd de afdeling Juridische Zaken.
- Gebruik de computersystemen van het Maasstad Ziekenhuis alleen zakelijk.
- Raadpleeg patiëntinformatie alleen als je een behandelrelatie hebt met de patiënt.
- Vertrouwelijke medewerkersgegevens mag je alleen inzien als je een relevante werkrelatie met die persoon hebt.
- Denk na over wat je zegt, tegen wie, en waar. Probeer alleen te overleggen op plaatsen waar anderen geen persoonlijke of vertrouwelijke informatie kunnen opvangen.
- Laat medische of vertrouwelijke informatie nooit onbeheerd achter. Berg deze informatie direct na gebruik op (clear desk policy).
- Stop vertrouwelijke papieren na gebruik in de daarvoor bestemde afgesloten papiercontainer. Het wordt dan op de juiste manier afgevoerd.
- **Let op!** Het gebruik van informatiesystemen wordt in een logbestand bijgehouden. Het doel van deze logging is om het gebruik van onze informatiesystemen te controleren. Je kunt achteraf worden aangesproken op verkeerd gebruik (met eventuele consequenties),

In de tekst wordt gesproken over gevoelige of vertrouwelijke informatie. Hiermee bedoelen we medische of persoonsgegevens van patiënten, werk gerelateerde of persoonsgegevens van medewerkers of bedrijfsgevoelige gegevens die schade kunnen toebrengen aan patiënten, medewerkers of de naam van het Maasstad Ziekenhuis.

Verwerk en gebruik gegevens op de juiste manier

- Beveilig gegevens altijd volgens de 'Beveiligingsinstructies' van het Maasstad Ziekenhuis.
- Verzamel alleen bedrijfs- en persoonsgegevens waarvan je weet dat je ze op van je takenpakket mag verzamelen. Met middelen die je door het Maasstad Ziekenhuis ter beschikking zijn gesteld.
- Verzamel alleen gegevens die compleet, correct en up-to-date zijn.
- Informeer de patiënt of medewerker over waarom en waarvoor de gegevens verzameld worden. Zorg dat er, indien nodig, toestemming is gevraagd door jou of een collega.
- Geef alleen toegang tot patiënt- of persoonsgegevens aan derden wanneer dit deel uitmaakt van je takenpakket.
- Geef alleen toegang tot gegevens aan derden als de patiënt of medewerker uitdrukkelijk toestemming heeft gegeven.
- Geef derden alleen toegang wanneer er een wettelijke, of contractuele verplichting is.
- Gebruik bij het versturen van medische- en/of bedrijfsinformatie veilige media die door het Maasstad Ziekenhuis aangeboden of aanbevolen worden.
- Zorg dat de persoonsgegevens die je nodig hebt altijd beschermd zijn tegen verlies, diefstal en veranderingen.
- Zorg dat de verzamelde persoonsgegevens niet langer worden bewaard dan nodig is.
- Verwijs personen die hun privacyrechten willen uitoefenen (het recht op inzage, correctie en verwijderen of gegevensoverdraagbaarheid) naar de privacyverklaring op de website van het Maasstad Ziekenhuis of de afdeling Juridische Zaken.



Gebruik patiëntinformatie alleen voor het uitoefenen van je functie.

Gebruik ICT-middelen zorgvuldig

- Gebruik je Maasstad Ziekenhuis account niet privé en je privé account niet zakelijk.
- Je gebruikersnaam en wachtwoord zijn strikt persoonlijk. Leen deze nooit uit (ook niet aan een collega die je vertrouwt). Jij bent altijd verantwoordelijk voor het gebruik van je account en de daarbinnen uitgevoerde acties.
- Kies een veilig wachtwoord en wijzig dit regelmatig. Houd je hierbij aan het 'Wachtwoordbeleid' op Zenya.
- Vergrendel de computer áltijd als je de werkplek verlaat (clear screen policy).
- Sluit je computer aan het eind van de werkdag af.
- Print documenten áltijd zelf en laat ze niet liggen bij de printer of 'multifunctional'.
- Open of installeer nooit software of bestanden die je niet vertrouwt. Laat software áltijd installeren door ICT via een digitale melding.
- Gebruik mobiele apparatuur (smartphone, tablet) en informatiedragers (USB stick) zorgvuldig.
- Zakelijke mobiele apparatuur is primair bedoeld voor het uitoefenen van je functie. Voor het gebruik van privé mobiele apparatuur voor zakelijke doeleinden gelden voorwaarden. Zie hiervoor ons beleid 'Mobiele apparatuur'.



Gebruik internet alleen voor het uitoefenen van je functie.

Ga bewust om met internet, e-mail, social media en telefoon.

- Internetgebruik
 - Het downloaden en versturen van informatie via internet is kwetsbaar. Beperk internetgebruik tot het noodzakelijke en download alleen bestanden die je vertrouwt.
 - Gebruik internet alleen voor het uitoefenen van je functie.
 - Zorg dat je de richtlijn **'Internet-en e-mail gebruik binnen het Maasstad Ziekenhuis'** op Zenya kent.
- Beeldopnamen
 - Het is niet toegestaan zonder toestemming foto's of filmpjes van jou, andere medewerkers, patiënten of bezoekers te maken. Meer informatie vind je in de folder **'Rechten en plichten'** op de website van het Maasstad Ziekenhuis.
 - Medische en bedrijfsinformatie vanaf een beeldscherm of papier opnemen en opslaan is niet toegestaan.
- E-mails en bijlagen
 - Gebruik voor het versturen van vertrouwelijke informatie de 'secure mail' optie aangeboden door het ziekenhuis. Indien 'secure mail' niet mogelijk is, beveilig bijlagen dan met een wachtwoord.
 - Open nooit bijlagen in e-mails van onbekende afzenders en/of bijlagen die je niet helemaal vertrouwt.
- Social media
 - Plaats nooit patiënt- of gevoelige informatie over het Maasstad Ziekenhuis op social media als Facebook, LinkedIn en Twitter. Jij bent zelf verantwoordelijk voor eventuele consequenties.
 - Benut de kansen van social media voor de promotie van het ziekenhuis.
 - Garandeer hierbij onze vertrouwelijkheid en vermeld geen patiënt- of persoonsinformatie.
 - Denk bij het versturen of posten aan de mogelijke gevolgen voor patiënten, ziekenhuis etc.
 - Blijf beleefd en oordeel nooit. Toon respect.
 - Blijf bij je eigen vakgebied en deskundigheid.
 - Neem je verantwoordelijkheid en ga bewust om met social media.
 - Zie ook het **'Beleid Social media code'** op Zenya.
- Telefoon
 - Verstuur nooit medische en/of bedrijfsinformatie via een medium zoals WhatsApp, Messenger of sms. Gebruik de middelen die worden aangeboden vanuit het ziekenhuis.

Voorkom ongeautoriseerde toegang tot je werkplek

- Laat waardevolle, persoonlijke of risicovolle (bedrijfs)eigendommen nooit onbeheerd achter. Ook niet als je maar even de ruimte verlaat.
- Berg eigendommen altijd op in de daarvoor bestemde, af te sluiten opbergruimtes.
- Doe, indien mogelijk, de deur van je werkplek op slot als je deze verlaat.
- Draag je personeelspas goed zichtbaar.
- Leen je personeelspas, sleutels of Maasstad Ziekenhuis bedrijfsmiddelen nooit uit aan onbevoegden.
- Laat geen onbekenden mee naar binnen lopen op een afdeling die normaliter alleen toegankelijk is voor personeel.
- Spreek onbekenden op de afdeling vriendelijk aan. Wees gastvrij en vraag of je ze kunt helpen, voor wie ze komen en begeleid ze tot aan hun bestemming.
- Zorg dat leveranciers en stagiairs die op de werkvloer actief zijn altijd een bezoekerspas halen.
- Vertrouw je een situatie niet? Informeer een collega, je leidinggevende of bel de Beveiliging T: 5555 (spoed) of T: 4000 (geen spoed).

Leen nooit je gebruikersnaam en wachtwoord uit



Wees continu alert op onveilige situaties

- Bespreek zaken die je niet vertrouwt met een collega of je leidinggevende en bepaal samen welke actie je onderneemt.
- Wijs collega's op onveilig handelen en onveilige situaties.
- Houd je aan deze gedragsregels. Zo waarborg je de privacy van patiënten en collega's.
- Heb je ideeën voor verbeteringen? Geef deze door aan je leidinggevende of meldt dit direct via het Digitaal Meldpunt.

Spreek collega's aan op onveilig handelen

Volg de instructies voor het correcte en veilig gebruik van informatiesystemen

- Volg de juiste trainingen voor het gebruik, of beheer, van informatiesystemen en medische hulpmiddelen.
- Voor bepaalde voorzieningen is training en toetsing vereist voordat toegang tot de voorziening wordt gegeven, bijvoorbeeld de training HiX.
- De instructie of training is erop gericht het systeem adequaat te leren gebruiken en fouten in het gebruik te voorkomen. De training kan bestaan uit een handleiding, instructie of training op de werkplek. Al dan niet afgesloten met een toetsing.
- Als de training niet wordt aangeboden, vraag hier dan zelf om bij je leidinggevende.

Meld incidenten

Tijdens je werk kun je helaas te maken krijgen met verschillende (dreigende) incidenten. Meld incidenten, of bijna incidenten, altijd. Naast je eigen veiligheid, wordt de informatie gebruikt om de veiligheid van het ziekenhuis te verbeteren.

Meld incidenten op de juiste manier

- Datalek of informatiebeveiligingsincident
 - Meld incidenten omtrent een mogelijk datalek of informatiebeveiligingsincident via **T: 3880** of 'digitaal melden - Datalek melden' (op **Digitaal Meldpunt**).
- ICT-meldingen
 - Meld ICT storingen of incidenten bij de ICT-Servicedesk via **T: 3880** of 'digitaal melden - ICT Melding maken' (op **Digitaal Meldpunt**).
- Medewerker incident melden: MIM
 - Meld incidenten waar medewerkers tijdens de uitvoering mee te maken krijgen altijd via 'digitaal melden - MIM melding maken' (op **Digitaal Meldpunt**).
- Veilig incident melden: VIM
 - Meld patiënt gerelateerde (bijna) incidenten altijd via 'digitaal melden - VIM melding maken' (op **Digitaal Meldpunt**).
- Fysieke beveiliging, spoed
 - Bel bij dreigende, fysieke calamiteiten en verdachte of onveilige situaties de Beveiliging, **T: 5555**.
- Fysieke beveiliging, geen spoed
 - Meld incidenten als verlies, diefstal of beschadiging van (bedrijfs)eigendommen bij de Beveiliging via **T: 4000** of mail naar beveiliging@maasstadziekenhuis.nl. De afdeling geeft advies en kan helpen met het doen van aangifte.



Meld incidenten,
of bijna incidenten, altijd!

Meer weten?

Op InfoMaasie en Zenya vind je meer informatie over het onderwerp 'informatiebeveiliging'. Ook vind je daar de beleidsdocumenten, richtlijnen die binnen Maasstad Ziekenhuis gelden en het privacyreglement. Daarnaast staat in je contract en de Cao Ziekenhuizen informatie over de geheimhouding van vertrouwelijke gegevens.

Heb je vragen en/of suggesties, neem dan contact op met de Information Security Officer, T: (010) 291 36 85.



Maasstad Ziekenhuis
Maasstadweg 21
3079 DZ Rotterdam

T: (010) 291 19 11
E: info@maasstadziekenhuis.nl
I: www.maasstadziekenhuis.nl

**MAASSTAD
ZIEKENHUIS**

een santeon ziekenhuis

