Gedragscode veilig gebruik van informatiemiddelen

1. Doel

In ons werk gebruiken voortdurend informatie om samen te zorgen voor kwaliteit van leven: om goede zorg te leveren, onderwijs te geven, onderzoek te doen en om deze werkzaamheden te ondersteunen. Het gaat daarbij om allerlei soorten informatie:

- persoonsgegevens van patiënten, medewerkers en anderen;
- informatie over onze eigen werkzaamheden;
- informatie van organisaties waarmee we samenwerken zoals huisartsen en andere zorginstellingen.

Alle patiënten, onze medewerkers en collega-zorginstellingen gaan ervanuit dat we zorgvuldig omgaan met die informatie en ook met de computersystemen waarop we die informatie gebruiken.

Het St. Antonius Ziekenhuis moet deze informatie daarom beschermen. Daarbij houden we wel rekening met het risiconiveau. Dit risico hangt samen met onze wettelijke plichten, de waarde, het belang en gevoeligheid van deze informatie. Ook houden we rekening met andere belangen, zoals het leveren van goede zorg en de service die we onze patiënten bieden.

We moeten hier keuzes in maken. Daarom leggen we helder vast wat wel en niet is toegestaan en lichten we onze medewerkers voor.

Ook moet duidelijk zijn hoe de organisatie kan controleren of iedereen zich aan deze afspraken houdt en wat de gevolgen zijn bij overtredingen.

Dit document geeft praktische uitleg hierover, dient als bijlage bij het arbeidscontract en is de bron van ander voorlichtingsmateriaal.[1]

Meer informatie waaronder het hoofdbeleid gegevensbescherming en informatiebeveiliging en over specifieke situaties is te vinden op Kwaliteitsnet. Deze bevat ook de meest recente versies van alle documenten.

2. Toepassingsgebied

Dit beleid is van toepassing op:

Informatie	Alle digitale en papieren informatie die je verwerkt binnen de organisatie. Met verwerken bedoelen we: aanmaken, opslaan, wijzigen, versturen en verwijderen.
Systemen	Alle applicaties, ICT-systemen, apparatuur, voorzieningen en werkplekken in de organisatie en (erbuiten) die je gebruikt voor je werk.
Personen	Iedereen die in opdracht van het St. Antonius Ziekenhuis werkzaam is op een van de locaties van het ziekenhuis (of op afstand). Dit betreft dus niet alleen personeel in dienstverband maar ook medisch specialisten, leerlingen, studenten, arts-assistenten, stagiaires, vrijwilligers, externe werknemers en interim medewerkers.

In gevallen waarin we samenwerken met mensen en systemen buiten het St. Antonius Ziekenhuis proberen we:

- zoveel mogelijk onze eigen afspraken na te komen;
- anders afspraken te maken, zodat informatie minstens zo goed beveiligd is.

[1] Dit document vervangt in de bijlage bij het arbeidscontract de documenten “hoofdbeleid gegevensbescherming en informatiebeveiliging” en “Gedragscode gebruik ICT-en communicatiefaciliteiten”.

Gedragscode veilig gebruik van informatiemiddelen

Beleid

2.1. Het belang van informatiebeveiliging

Informatiebeveiliging gaat over de *beschikbaarheid, integriteit en vertrouwelijkheid* van gegevens.
Informatiebeveiliging is:

- de verantwoordelijkheid van ons allemaal en niet alleen van de ICT-beheerders;
- een integraal (onlosmakelijk) onderdeel van de patiëntenzorg.

Een patiënt is niet tevreden als:

- de operatie is uitgesteld omdat de ICT is uitgevallen (beschikbaarheid van informatie).
- de labverslagen fouten bevatten waardoor er een verkeerde diagnose is gesteld (integriteit van informatie).
- de operatie is geslaagd maar het patiëntendossier is ingezien door onbevoegden (vertrouwelijkheid van informatie).

Daarnaast is privacy een *grondrecht*: patiënten, maar ook medewerkers hebben er recht op dat het ziekenhuis op een zorgvuldige manier omgaat met hun persoonsgegevens.

Slechte informatiebeveiliging heeft natuurlijk gevolgen voor de patiënt, maar ook voor jezelf, je team, afdeling, het ziekenhuis en uiteindelijk de hele regio en de samenleving.
Denk hierbij aan: uitval van systemen en medische zorg met mogelijk fatale gevolgen, reputatieschade door media-aandacht, financiële gevolgen, maar bijvoorbeeld ook boetes van toezichthouders.
Bij ernstige overtredingen neemt het St. Antonius Ziekenhuis ook disciplinaire maatregelen volgens de algemene gedragscode, tot en met ontslag.

Doelstelling 1.	Je begrijpt dat we informatie moeten beschermen en kent de gevolgen als we dat niet doen.

2.2. Welke middelen gebruik je

Gebruik alleen goedgekeurde middelen

We gebruiken voor ons werk veel ICT-systemen, denk bijvoorbeeld aan het EPD, de e-mail en je werktelefoon. Maar je mag niet alles gebruiken: sommige systemen zijn onvoldoende veilig. Maak daarom alleen gebruik van apps of informatiesystemen die door het St. Antonius Ziekenhuis zijn aangeschaft en/of goedgekeurd (bijlage A en bijlage B). Twijfel je of een systeem is goedgekeurd, vraag dit na bij de ICT Servicedesk.
NB: Leidinggevenden kunnen je niet dwingen om gebruik te maken van niet goedgekeurde middelen.

Doelstelling 2.	Je gebruikt alleen goedgekeurde middelen voor je werk.

2.3. Waarvoor en hoe gebruik je middelen

Gebruik voor bedrijfsgerelateerde doelstellingen

Je mag informatiemiddelen gebruiken voor je werk, dus voor patiëntenzorg, onderwijs, onderzoek en ondersteunende diensten. Beperkt privégebruik van middelen zoals computers, telefoons, printers en e-mail mag zolang het:

- de continuïteit van de bedrijfsvoering niet belemmert;
- niet ten koste gaat van de normale werkzaamheden;
- niet voor hoge kosten zorgt;
- niet commercieel-privé van aard is;
- niet strijdig is met de andere principes.

NB: het gebruik voor privédoeleinden is natuurlijk toegestaan als hier aparte afspraken over zijn: bijvoorbeeld werktelefoons hebben zowel een privé-omgeving als een werkomgeving.

Gebruik in overeenstemming met fatsoensnormen en wettelijke bepalingen

Je respecteert de algemene normen en waarden en wettelijke bepalingen. Niet toegestaan zijn:

- diefstal, fraude, valsheid in geschrifte, ongeautoriseerd binnendringen in computersystemen van het St. Antonius Ziekenhuis of derden;
- schending van auteursrechten, waaronder het maken van illegale kopieën van software of installatie van software zonder dat je een gebruikslicentie hebt;
- discriminatoir of pornografisch materiaal te vervaardigen, downloaden, gebruiken, tonen of verspreiden, waaronder teksten, afbeeldingen, geluid- of video-opnames.

- andere activiteiten waarvan je redelijkerwijs kunt begrijpen dat het St. Antonius Ziekenhuis zich hiermee niet kan verenigen en/of betrokkenheid van het St. Antonius Ziekenhuis bij dit materiaal de eer en goede naam van het St. Antonius Ziekenhuis schaadt.

Houd je verder aan de gedragscode van de beroepsgroep die op jou van toepassing is (zoals de KNMG en de V&VN).

Doelstelling 3.	Je weet dat beperkt privégebruik van middelen is toegestaan zolang niemand er last van heeft en je je houdt aan de fatsoensnormen en de wet.

2.4. Informatie classificeren en labelen

Welke soorten informatie hebben we

Binnen het ziekenhuis gebruiken we 4 soorten informatie:

- **Publiek:** deze mag je delen met de hele wereld.
- **Intern:** deze mag je delen met de hele organisatie.
- **Vertrouwelijk:** alleen een bepaalde groep medewerkers mag deze informatie inzien. Verdere verspreiding levert problemen op.
- **Geheim:** deze informatie is zeer vertrouwelijk. Verdere verspreiding kan veel schade veroorzaken.

	Soort informatie of document			
	Publiek	Intern	Vertrouwelijk	Geheim
Risico	Laag	Midden	Hoog	Zeer hoog
Voorbeelden	Publiek beschikbare informatie op internet: • website informatie • flyer- en marketing-informatie	Informatie bedoeld voor interne documentatie en communicatie: • beleidsdocumenten en protocollen • nieuwsbrieven	Gevoelige informatie voor beperkte groep personen: • Auditrapporten • Investeringsplannen • concept jaarverslagen • medische dossiers en medisch inhoudelijke gegevens[2] • ontwerpen van systemen en beveiligings-mechanismen	Kritieke, strategische informatie of medische gegevens voor beperkte groep personen: • prijsinformatie gebruikt bij onderhandelingen

Labelen van informatie

In informatiesystemen zoals het EPD geven we niet aan wat voor informatie het betreft, maar dat moet wel voor documenten: zijn deze publiek, intern, vertrouwelijk of geheim? Door informatie te labelen weet je beter hoe je het moet beschermen en wat het risico is.

De eigenaar van het document is verantwoordelijk voor de correcte classificatie.
Informatie behoudt in principe de classificatie die het heeft gekregen. Bij het aanpassen van een document heroverweeg je de classificatie en pas je die zo nodig aan.

NB: Sommige documenten gebruiken we zo vaak dat we hier aparte afspraken over hebben. Labeling van deze documenten is aanbevolen maar niet verplicht.

De vuistregel is dat je tenminste moet labelen als er een kans is op misverstanden en incidenten.

[2] Zie A.8.2.1 Classificatie van informatie: Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren dergelijke gegevens op uniforme wijze als vertrouwelijk te classificeren.

	Soort informatie of document			
	Publiek	Intern	Vertrouwelijk	Geheim
Plaatsing van het label	Labelen nooit verplicht	Het label moet tenminste op de eerste pagina van een document aanwezig zijn.	Het label moet tenminste op de eerste pagina van een document aanwezig zijn.	Het classificatieniveau 'geheim' moet aanwezig zijn: • op de voorpagina zonder inhoudelijke tekst; • in de voettekst van alle pagina's.
Labeling niet verplicht bij	-	Tekst of document op intranet, beleidsdocument	E-mail Medische gegevens (zowel digitaal als geprint) Gedeelde folders	-

Doelstelling 4. Je kent de gevoeligheidslabels (publiek, intern, vertrouwelijk en geheim) en weet wanneer je labels moet plaatsen.

2.5. Incident herkennen en melden

Tijdens het werk kun je te maken krijgen met verschillende soorten incidenten.

Datalekken

Een datalek is een gebeurtenis waarbij persoonsgegevens verloren zijn gegaan, bij een verkeerde gebruiker of bij een verkeerde persoon buiten de organisatie terecht zijn gekomen of onterecht zijn gewijzigd. Datalekken meld je zo snel mogelijk via de werkplek (Start > Datalek melden).

ICT-incidenten

ICT-incidenten zijn bijvoorbeeld phishing mails, virussen, uitval van ICT, datalekken, gestolen of verloren laptops etc. ICT-incidenten meld je bij de ICT Service Desk.

Phishing

Bij phishing probeert een oplichter te 'hengelen' naar persoonlijke gegevens van iemand (zoals wachtwoorden, persoonsgegevens) of je over te halen om handelingen te doen (bijvoorbeeld snel geld overmaken). Phishing kan voorkomen via mail, chat, videobellen en telefoon. Het is soms lastig om phishing te herkennen. Een paar vuistregels:

- Wees extra alert zodra iemand snel iets wil en met gezag druk uitoefent om iets te doen wat mogelijk risicovol is (nu snel geld overmaken, snel gegevens nodig t.b.v. een patiënt, je account wordt nu geblokkeerd als je geen actie onderneemt).
- Maak voor risicovolle processen zoals betalingen en wijzigingen van bankrekeningnummers altijd gebruik van bestaande procedures.
- Klik niet zomaar op links van onbekende afzenders.
- Identificeer je contacten volgens het beleid op Kwaliteitsnet (bijvoorbeeld patiëntidentificatie)
- Heb je twijfel over de afzender, bel of mail terug via een kanaal dat je kent zodat je meer zekerheid hebt met wie je te maken hebt (bijvoorbeeld een bekend e-mailadres).

Voor e-mail geldt dat externe mail (van buiten het St. Antonius Ziekenhuis) altijd herkenbaar is aan een waarschuwing dat het om externe mail gaat.

Phishing-incidenten meld je altijd bij de ICT Servicedesk.

Overige incidenten

Deze incidenten meldt je bij Facilitaire Zaken:

- verloren of gestolen St. Antonius-passen;
- problemen met het sluiten van deuren;
- diefstal van niet-ICT-middelen.

Doelstelling 5.	Je kunt datalekken, phishing en andere informatiebeveiligingsincidenten herkennen, weet hoe te handelen en hoe je deze meldt.

2.6. Bedrijfscontinuïteit

Het St. Antonius Ziekenhuis is sterk afhankelijk van ICT voor patiëntenzorg, onderwijs en onderzoek. Helaas is er altijd een kans dat de ICT uitvalt. Daarom moet je jezelf (en je team, afdeling, eenheid) voorbereiden op uitval van ICT, mogelijk langdurig. Zorg ervoor dat:

- je weet wat de afgesproken noodprocedures zijn;
- je oefent met deze noodprocedures.

Doelstelling 6.	Je begrijpt dat het ziekenhuis afhankelijk is van ICT en je oefent met de noodprocedures.

2.7. Fysieke beveiliging

Je werkt in een open organisatie waar bezoekers en patiënten veel bewegingsvrijheid hebben. Daarom blijf je alert en neem je fysieke beveiligingsmaatregelen.

Indeling in zones

In het ziekenhuis hebben we vier soorten beveiligingszones:

- publiek: toegankelijk voor bezoekers.
- vleugel: toegankelijk voor bezoekers tijdens kantoortijden / bezoekuren.
- kantoorruimte: toegankelijk voor (alle) medewerkers.
- extra beveiligde ruimte: toegankelijk voor medewerkers met juiste autorisatie.

Het is belangrijk dat je weet in welke zone je werkt, omdat de risico's en de beveiliging per zone verschillen.

Kantoorruimte

In kantoorruimtes:

- Pas het clear-desk principe toe: zorg ervoor dat je bureau leeg is en blijft.
- Pas het clear screen principe toe: vergrendel je scherm als je je werkplek verlaat.
- Hang geen vertrouwelijke stukken op prikborden (actielijsten met problemen, notulen etc.).
- Laat geen sleutels in sloten zitten en verstop ze ook niet in je kantoor. Neem ze mee of berg ze op in een sleutelkastje.
- Verplaats je werkplek en je systemen niet zelf, maar laat dit over aan de ondersteunende diensten.
- Bij het verlaten van de werkplek en tenminste aan het einde van je werkdag of dienst:
  - Berg vertrouwelijke (papieren) documenten op in kasten of lades en sluit deze af.
  - Leeg open papierbakken en gooi al het papier in de afgesloten papierbakken.
  - Doe je deur op slot.
  - Sluit alle ramen.

	Soort informatie of document		
	Publiek	Intern	Vertrouwelijk
Dagelijks gebruik	Geen beperkingen	• Vrij gebruik op elke locatie en in elke ruimte die niet toegankelijk is voor bezoekers of waar bezoekers niet mee kunnen kijken. • Toepassen van clear screen bij het verlaten van de werkplek. • Fysiek afsluiten van werkplekruimte bij het verlaten (indien mogelijk).	• Intern + Bekijken van document mits onbevoegden niet kunnen meekijken. • Toepassen van clear desk bij het verlaten van de werkplek of aan het einde van de dag op basis van risico. • Wissen van whiteboard na gebruik.

	Soort informatie of document		
Opslag fysiek[3]	Geen beperkingen	Opslag in ruimtes die alleen toegankelijk zijn voor medewerkers of 24x7 worden bemand.	• Zie Intern + opslag in afgesloten kast. • Niet achterlaten in publieke of risicovolle ruimtes (in auto's etc.)
Vernietiging fysiek	Geen beperkingen	Gebruiken van papiercontainer voor vertrouwelijke documenten	Zie Intern

Bespreken van vertrouwelijke informatie

In semipublieke ruimtes (gemengde zone publiek / / kantoorruimte):

- Probeer geen NAW-gegevens te noemen als anderen dat kunnen horen.
- Voer geen vertrouwelijke gesprekken daar waar anderen mee kunnen luisteren.

Aanspreken

- Spreek bezoekers / onbekenden aan als ze zich begeven op plekken waar dit niet nodig lijkt te zijn ("kan ik u helpen?").
- Let op dat er geen mensen achter je aanlopen als je een deur opent - dragen ze zelf een pas en hebben ze een reden om hier te zijn?

Antonius Pas

- Draag je pas zichtbaar, zodat je herkenbaar bent.
- Leg je pas niet neer op je bureau, hij geeft toegang tot deuren en systemen en je kunt hem makkelijk vergeten.
- Leen je pas niet uit.

Doelstelling 7.	Je begrijpt het belang van fysieke beveiliging en je zorgt dat informatie ook fysiek veilig is.

2.8. Digitale beveiliging

Clear screen

- Pas het clear-screen principe toe: vergrendel je scherm bij het verlaten van je werkplek (d.w.z. je verlaat de ruimte waarin je werkt en hebt er geen direct zicht meer op). Op deze manier hebben derden bij jouw afwezigheid geen toegang tot vertrouwelijke informatie.

Wachtwoord en accountbeveiliging

- Houd de gegevens van je medewerkersaccount voor jezelf. Geef nooit jouw wachtwoord (of Antonius Pas) aan anderen te leen.
- Omgekeerd: log ook niet in op accounts van anderen.
- Wijzig je persoonlijk wachtwoord regelmatig volgens het geldende beleid:
  - Zorg voor een sterk wachtwoord dat niet makkelijk te raden is.
  - Gebruik nooit dezelfde wachtwoorden voor privé- en werkaccounts.

Geheimhouding en vertrouwelijkheid

- Laat anderen niet meelezen op je scherm.
- Geef persoonsgegevens en andere vertrouwelijke informatie alleen aan collega's of relaties die hiertoe bevoegd zijn deze nodig hebben;

Goedgekeurde middelen

- Bewaar informatie alleen op systemen en in applicaties die door het ziekenhuis zijn goedgekeurd.
- Maak geen gebruik van USB-sticks voor de opslag van vertrouwelijke gegevens.

[3] Inclusief de opslag van datadragers; Zie fysieke en omgevingsbeveiligingsbeleid voor de exacte eisen aan ruimtes.

	Soort informatie of document			
	Publiek	Intern	Vertrouwelijk	Geheim
Opslag digitaal	-	Opslag op systemen binnen de organisatie of netwerk	Intern + opslag op systeem dat afgeschermd is per afdeling of team	Vertrouwelijk + waar mogelijk document versleutelen met wachtwoord
Logging	-	-	Voor medische data: logging van alle bewerkingen.	Logging van alle bewerkingen.
Vernietiging	Normaal verwijderen van bestand	Normaal verwijderen van bestand	Normaal verwijderen van bestand	Voor versleutelde bestanden: • Wijzingen van wachtwoord naar willekeurige tekens. • Daarna verwijderen van bestand en legen van prullenbak.

Doelstelling 8. Je begrijpt wat je moet doen om onze informatie en informatiesystemen veilig te houden en voorkomt incidenten.

2.9. Thuiswerkplekken

Begrijp de extra risico's:
Een thuiswerkplek is geen volledig beheerde werkplek waarop je ondersteuning kunt krijgen. Wees je bewust van de extra risico's, zoals:

- Kapotte hardware (telefoon/PC/laptop/tablet);
- Internet- en telefoonstoringen;
- Softwareproblemen;
- etc.

Heb je tijdkritische werkzaamheden? Denk dan vooraf na over hoe je bovenstaande risico's kunt beperken door een alternatief te regelen.

Werkplekinrichting

- **Fysieke werkplekinrichting thuis:** zorg dat je een werkplek hebt waar niet iedereen kan meekijken of meeluisteren (buren, familie). Vergeet ook je eigen apparatuur hierbij niet (smart TVs, speakers).
- **Digitale thuiswerkplek (PC of laptop):** werk vanaf een systeem dat helemaal geüpdatet is. Internet zoveel mogelijk via je eigen internetverbinding: maak je bij het thuiswerken gebruik van het internet? Doe dit dan zoveel mogelijk via je eigen internetverbinding en niet binnen de thuiswerkplek-sessie. Zo ontlast je het netwerk. Dat wil zeggen:
    1. Maak binnen een thuiswerkplek-sessie zo min mogelijk gebruik van internet, maar surf op het internet via jouw eigen internetverbinding.
    2. Werk je thuis via je thuiswerkplek en wil je videobellen? Doe dat dan zoveel mogelijk via je eigen internetverbinding en niet binnen de thuiswerkplek-sessie.
    3. Sluit browservensters na gebruik af.

Gebruik van eigen apparatuur
Het gebruik van eigen (rand) apparatuur zoals een laptop of PC is toegestaan met een aantal voorwaarden:

- Je maakt alleen gebruik van goedgekeurde applicaties zoals de thuiswerkplek.
- Je bewaart geen informatie en documenten van het St. Antonius Ziekenhuis op jouw apparatuur.
- De apparatuur krijgt updates van de leverancier (Apple / Microsoft).
- Je verricht geen handelingen die de beveiliging verzwakken of tenietdoen waaronder het gebruik van illegale / schadelijke software.
- De apparatuur is voldoende beveiligd (wachtwoorden, regelmatig updaten, antivirus etc., overeenkomstig de eisen van het St. Antonius Ziekenhuis).

- Virtuele assistent software (Google Assist, Apple Siri, Amazon Alexa) staat uitgeschakeld in werksituaties.
- Je maakt geen gebruik van persoonlijke back-ups in de cloud voor gegevens van het St. Antonius Ziekenhuis.
- Je beoordeelt en borgt als eigenaar van het systeem zelf dat het systeem voldoende krachtig is om de werkzaamheden naar behoren te verrichten. Hierbij gaat het bijvoorbeeld om netwerksnelheid en -capaciteit, voldoende algemene verwerkingssnelheid en een scherm met voldoende kwaliteit voor de weergave van medische (radiologische) toepassingen;
- Alle opgeslagen data is versleuteld.

Overig

Let verder op de volgende punten:

- Stuur geen werkbestanden naar je privé-e-mailadres om thuis aan te kunnen werken.
- Download geen bestanden vanaf je werk-webmailbox op je thuis-PC.
- Neem geen bestanden mee naar huis op USB-stick.

Omgaan met papieren documenten

Neem zo min mogelijk papieren documenten mee. Heb je deze wel, pas dan onderstaande regels toe:

	Soort informatie of document		
	Publiek	Intern	Vertrouwelijk of geheim
Thuiswerken	-	Tijdelijke fysieke opslag op thuislocatie van kopieën toegestaan.	• Thuiswerkplek is op aanvraag beschikbaar, gegevens niet opslaan op eigen systemen van medewerker (laptop / PC). • Gegevens alleen fysiek opslaan in geval van zwaarwegende redenen. • Papieren informatie alleen op het werk laten vernietigen.

Onderweg

- Voorkom diefstal: laat geen pasjes, telefoons, computers of vertrouwelijke documenten onbeheerd achter in je auto.

Doelstelling 9. Je beveiligt je thuiswerkplek.

2.10. Communicatie

Principe: houd het netjes

Informatie kan door diverse oorzaken uitlekken naar andere medewerkers en organisaties. In het ergste geval kunnen je berichten in bulk op internet gepubliceerd worden.
Wees je hiervan bewust en neem voorzorgsmaatregelen:

- Communiceer formeel en overeenkomstig de gedragscode, zodat je niet persoonlijk in verlegenheid gebracht wordt bij publicatie door te persoonlijk of grof taalgebruik. Blijf professioneel, zeker bij ernstige incidenten of problemen.
- Wees voorzichtig met woorden die juridische consequenties kunnen hebben (het gebruik van termen als “niet-compliant”, “in strijd met wet- en regelgeving”), specifiek als de beoordeling hiervan niet noodzakelijk is uit hoofde van je functie.

Gebruik het meest veilige communicatiemiddel

Zijn er meerdere communicatiemogelijkheden, gebruik dan het meest veilige communicatiemiddel. Speciaal voor de communicatie met patiënten staan hieronder wat handreikingen, telkens is de meest veilige keuze al eerste vermeld.

- Gebruik je e-mail? Via deze link https://relay-domains.ezorg.nl/domains-extra.txt kun je controleren of de ontvangende partij aangesloten is op Zorgmail. Is dat het geval, dan gaat veilig mailen automatisch.
- Verstuur als het kan niet de informatie zelf maar alleen een link ernaartoe. Zo zijn er minder kopieën van de informatie.

Gedragscode veilig gebruik van informatiemiddelen

Directe en persoonlijke communicatie

Middel	Keuze	Uitleg
Persoonlijk gesprek	1e	Niet in publieke ruimtes
Telefoon	2e	Terugbelspreekuur etc.
Videoconferencing	3e	Voor specifieke applicaties

Versturen van (patiënt)gegevens

Middel	Keuze	Uitleg
Online patiëntenportaal Mijn Antonius	1e	Dit mag altijd.
Verzendknop veilige e-mail	2e	Als het patiëntenportaal niet werkt.
Versleuteld als bijlage (met 7 zip)	3e	Als de veilige e-mail optie niet werkt.
Gewoon mailen	4e	Als er geen andere opties zijn[4], met toestemming van de patiënt.

Let op dat je met de juiste persoon communiceert

Bij digitale communicatie bestaat het risico dat informatie bij een verkeerde afzender terechtkomt of dat een bericht afkomstig is van een andere afzender dan je verwacht. Wees zorgvuldig en controleer dat je communiceert met de juiste ontvanger en/of verzender van een bericht. Bekijk het authenticatiebeleid en het patiëntidentificatiebeleid voor verdere uitleg.

	Soort informatie of document			
	Publiek	Intern	Vertrouwelijk	Geheim
Delen intern	-	Vrije te delen binnen de organisatie	Delen binnen betrokken afdelingen / teams	• Delen binnen betrokken afdelingen / teams. • Indien van toepassing: delen beperkt tot personen op de distributielijst
Delen extern	-	Uitwisseling met bekende relaties en partners wanneer nodig toegestaan onder geheimhoudingsverklaring / samenwerkingsovereenkomst	• Geheimhoudingsovereenkomst is nodig met externe organisatie. • Voor persoonsgegevens is verwerkersovereenkomst nodig. • Versleuteld versturen van bestand.	• Geheimhoudings-overeenkomst met externe organisatie en persoonlijke geheimhoudingsovereenkomst òf wettelijke basis voor gebruik. • Versleuteld versturen van bestand.

Communicatie via platformen voor informatie-uitwisseling

Partners, koepelorganisaties, klanten en leveranciers bieden vaak hun eigen platformen aan voor informatie-uitwisseling. Hiervoor gelden de volgende eisen:

- Voor losse samenwerkingsverbanden met professionals in de zorg (expertgroepen etc.) ben je zelf verantwoordelijk om de beveiliging van deze systemen te beoordelen en alleen documenten te plaatsen die gedeeld mogen worden volgens de eisen over informatiebeveiliging. Let speciaal op de aanwezigheid van een beveiligde verbinding en het beheer van toegangsrechten van aangesloten organisaties en personen.
- Voor samenwerking op meer structurele basis zoals met klanten en andere zorginstellingen kun je het beste overleggen met een informatiemanager.

Doelstelling 10. Je wisselt gegevens veilig uit met collega's, patiënten en anderen.

[4] Denk daarbij ook aan het versturen per post.

Gedragscode veilig gebruik van informatiemiddelen

2.11. E-mail en chat

Gedragsregels e-mail

- Het is niet toegestaan om:
  - gebruikersnamen en wachtwoorden te gebruiken die op niet reglementaire wijze verkregen zijn;
  - een e-mailadres van een andere gebruiker als afzender te gebruiken;
  - anoniem e-mail te versturen of e-mailberichten op enige wijze te vervalsen;
  - mailboxen van andere gebruikers te gebruiken anders dan met toestemming van de betrokkene;
  - e-mailberichten te ondertekenen met gebruikmaking van een andere naam.
- Open nooit zomaar bijlagen of links in e-mails van onbekende herkomst en meld verdachte e-mails (zie sectie 2.5).

Bewaren van (email) communicatie

Heb je belangrijke e-mails die als naslag bewaard moeten blijven voor de organisatie?
Laat deze niet in je persoonlijke mailbox staan maar sla deze elders op.
Je persoonlijke mailbox wordt namelijk verwijderd als je uit dienst gaat.
Je kunt mails op een aantal manieren bewaren, bijvoorbeeld:

- Verplaats ze naar een gedeelde e-mailbox;
- Bewaar ze als bestand (.eml) op een gedeelde netwerkschrijf;
- Bewaren de bijlagen van de e-mail.

NB: Voor e-mail zal je zelf een afweging moeten maken wat wel en niet bewaard moet worden. Als een e-mail bewaard moet worden (conform het retentiebeleid) moet je deze e-mail bij beëindiging van de werkrelatie overdragen.

Gedragsregels chatten

- WhatsApp is een middel dat we beperkt toestaan: Je mag het gebruiken voor informeel privégebruik en simpele onderlinge communicatie met andere medewerkers. Het is niet toegestaan om patiëntgegevens via WhatsApp te delen.
- Een goedgekeurd alternatief voor WhatsApp is de KPN Zorg Messenger App voor je telefoon. Je vindt deze in de App store door te zoeken op ‘Zorg Messenger’. Registreer jezelf met je werk-e-mailadres en gebruik de app vanaf je werktelefoon. De app is via de browser beschikbaar op: https://zm.kpnzorg.nl

Doelstelling 11. Je e-mailt en chat veilig.

2.12. Webbrowsen (Internet)

Gedragsregels internet

- Negeer geen veiligheidswaarschuwingen: let bij het invullen van formulieren op internet op dat de verbinding beveiligd is (het slotje).
- Bezoek geen sites waarvan je weet dat er mogelijk malware op aanwezig is of er illegale praktijken plaatvinden.

	Soort informatie of document		
	Publiek	Intern	Vertrouwelijk of geheim
Gebruik in vrij beschikbare online tooling zoals vertaaldiensten, zoekmachines en AI toepassingen	Vrij te gebruiken voor kortdurend gebruik (zoekfunctie/vragen) zolang informatie niet langdurig wordt opgeslagen.	Vrij te gebruiken voor kortdurend gebruik zolang informatie: • niet langdurig wordt opgeslagen; • de privacy van medewerkers en anderen niet schendt; • geen schade of verlies oplevert voor de organisatie (denk aan intellectueel eigendom).	Niet toegestaan.

Doelstelling 12. Je internet veilig en houdt je aan de regels voor gratis online diensten.

2.13. Videobellen

Het St. Antonius Ziekenhuis stelt middelen ter beschikking om te videobellen, zowel voor intern gebruik als voor communicatie met patiënten, andere zorgverleners en bijvoorbeeld leveranciers. Videobellen kan makkelijker en efficiënter zijn dan fysiek afspreken maar er zijn ook risico's aan verbonden. Zo kunnen anderen onbedoeld meeluisteren of meekijken, waardoor vertrouwelijke informatie in verkeerde handen komt.

Gedragsregels videobellen

- Plan je een videoconference: maak dan gebruik van de applicaties die het St. Antonius Ziekenhuis ter beschikking stelt. Gebruik geen gratis software die je zelf hebt geregistreerd. Je mag wel aansluiten bij videoconferences van andere organisaties mits zij zelf een contract hebben voor deze software.
- Controleer voordat je vertrouwelijke informatie uitwisselt dat alleen geautoriseerde personen in de videoconference aanwezig zijn. Maak zo nodig gebruik van de technische middelen om dit af te dwingen (pincodes, het vergrendelen van de videoconference, persoonlijke uitnodigingen etc. etc.)
- Deel vertrouwelijke stukken alleen vanaf je St. Antonius- werkplek; verstuur geen documenten naar privéapparatuur om deze te delen. Log zo nodig een tweede keer in vanaf je St. Antonius-werkplek om vanaf daar documenten te delen.
- Deel niet meer informatie dan nodig. Clear desk en clear screen zijn ook van toepassing op videoconferences. Bedenk dat deelnemers makkelijk een schermafdruk kunnen maken van de informatie of een foto met hun mobiele telefoon. Zo voorkom je informatielekken.

Voorafgaand aan de sessie:

- Ruim je bureaublad op.
- Sluit applicaties die je niet nodig hebt en voorkom dat applicaties je tijdens het geven van een presentatie pop-up berichten sturen.
- Als je gebruik gaat maken van een internetbrowser, wis je historie of open een nieuw 'incognitovenster'.

Bij het delen van je scherm:

- Veel videoconferencing-applicaties hebben de mogelijkheid om alleen een bepaald venster van een applicatie te delen in plaats van je hele bureaublad. Maak hier gebruik van.
- Ben je klaar met je presentatie? Stop dan ook met het delen van je scherm. Zo voorkom je dat je dit vergeet en later ongewild toch nog informatie deelt.

Doelstelling 13. Je videobelt veilig.

2.14. Telefonie

Gedragsregels werktelefoon

De belbundels zijn ruim maar niet onbeperkt. Beperk daarom de kosten waar mogelijk:

- Gebruik je telefoon niet als hotspot voor privégebruik.
- Neem geen commerciële diensten af: bel niet naar 0900/0906/0909-nummers en abonneer je ook niet op betaalde sms-diensten;
- Werk je langdurig op één plek en verbruik je veel data bijvoorbeeld voor videobellen? Maak dan waar mogelijk gebruik van beveiligde Wifi[5] in plaats van het mobiele telefonie netwerk.

Ben je je telefoon kwijt?

- Geef verlies of diefstal zo spoedig mogelijk door aan de ICT Servicedesk.
- Doe bij diefstal en verlies altijd aangifte bij de politie. Dit kan gewoon online.

Gebruik van een privételefoon en -nummer

Veel medewerkers hebben een werk- en een privételefoon en met eigen 06 nummer. In principe gebruiken we het werknummer voor werkgesprekken en het privénummer voor privégesprekken. Dat is belangrijk voor de organisatie: bij vertrek houdt het St. Antonius Ziekenhuis controle over de werknummers en kan niemand zich voordoen als een medewerker van het St. Antonius Ziekenhuis,

[5] Je herkent een beveiligd wifi-netwerk aan het slotje 🔒 dat erbij staat. Je moet dan een wachtwoord invoeren om verbinding te maken.

terwijl hij uit dienst is. Maar het is ook belangrijk voor jezelf: je kunt privé niet telefonisch lastig worden gevallen als je je privételefoonnummer niet deelt.

Voicemail
Spreek liever geen vertrouwelijke informatie in op de voicemail: veel gebruikers beveiligen hun voicemail niet goed. Is het niet nodig om voicemail te hebben voor je functie: zet deze uit.

Doelstelling 14. Je maakt veilig gebruik van je telefoon.

2.15. Het EPD

Het meest belangrijke informatiesysteem in het ziekenhuis is het EPD. Hier staan de gegevens van miljoenen patiënten. Daar moeten we zuinig mee omgaan. Een aantal basisregels hierbij zijn:

- Kijk alleen in dossiers als hier een noodzaak toe is vanuit je functie (een behandelrelatie of andere noodzaak).
- Zorg ervoor dat niemand kan meekijken.

Het is dus niet toegestaan om onbevoegd in andere dossiers te kijken, zelfs niet je eigen dossier (hiervoor gebruik je het patiëntenportaal).
Het is ook niet toegestaan in dossiers van vrienden en familie te kijken (ook niet met hun toestemming). Heb je inzage nodig omdat bijvoorbeeld een vader of moeder behandeld wordt in ons ziekenhuis? Regel dan toestemming hiervoor en bekijk het dossier vanuit het patiëntenportaal.

Doelstelling 15. Je maakt veilig gebruik van het EPD.

2.16. Je eigen rol

We wijzen je op je eigen rol bij het veilig houden van onze informatie. Zorg ervoor dat je jezelf scherp houdt en de regels blijft hanteren. Het volgende kan hierbij helpen:

- Wees niet kwetsbaar voor je eigen voorspellingen: denk niet “het gebeurt vast niet dat…”
- Durf elkaar aan te spreken op overtredingen. Begin met het gesprek aan te gaan: “Ik zie dat… herken je dat… is dat geen risico?”
- Herinner jezelf eraan dat:
    - je in deze organisatie werkt met zeer vertrouwelijke patiëntgegevens;
    - het ziekenhuis toegankelijk is voor iedereen;
    - bij ernstige nalatigheid of kwade opzet, sancties en disciplinerende maatregelen mogelijk zijn zoals in de gedragscode staat.
- Stel jezelf de vraag: wat betekent mijn handelen voor de **beschikbaarheid**, **integriteit** en **vertrouwelijkheid** van onze gegevens?
- Stel je voor dat iemand anders jouw taken zorgvuldig zou uitvoeren. Zou hij/zij dat op dezelfde manier doen?
- Kun je je acties aan anderen laten zien of uitleggen zonder te blozen?

Doelstelling 16. Je kent je eigen rol bij het veilig houden van informatie, de valkuilen daarbij en weet hoe je jezelf scherp kunt houden.

2.17. Toezicht, controle en privacy

Het St. Antonius Ziekenhuis voert controles uit op gebruik van de informatiesystemen en werkplekken. Dit zijn aan de ene kant normale en doorlopende controles bijvoorbeeld om te voorkomen dat er virussen meekomen met e-mails. Maar het St. Antonius Ziekenhuis kan ook gerichte controles uitvoeren, bijvoorbeeld na een melding van mogelijk misbruik of overtredingen van de afspraken. Concrete voorbeelden hiervan zijn controle op de rechtmatige toegang tot het EPD en excessief datagebruik op je mobiele telefoon. De procedures en ook mogelijke sancties kun je nalezen in de algemene gedragscode van het Antonius Ziekenhuis.

Borging en doorbreken van de privacy van medewerkers
Medewerkers werken normaliter onder persoonlijke accounts (werkplek, e-mail) bij hun werkzaamheden. De medewerker heeft hier recht op privacy maar niet tot elke hoogte. Leidinggevenden en anderen kunnen toegang krijgen tot deze gegevens indien:

- Dit noodzakelijk is voor ICT beheerswerkzaamheden;
- Deze toegang uitdrukkelijk is gedeeld door werknemer;

- Informatie in een informatiesysteem is opgeslagen waarbij de toegang gedeeld is (bijvoorbeeld een medisch systeem);
- Indien er sprake is van een dwingend bedrijfsbelang.

Doelstelling 17. Je weet dat het ziekenhuis toezicht houdt op de informatievoorziening, dat er bij zwaarwegende redenen inzage kan zijn in jouw bestanden en informatie en ook dat er sancties kunnen volgen op overtredingen van het beleid.

Besluitvoering en goedkeuring

Deze gedragsregels zijn opgesteld onder goedkeuring van de Raad van Bestuur. Het document wordt onderhouden door de eenheid HR, AR&C, I&I, FZ. Besluitvorming loopt via de bestuursadviescommissie gegevensbescherming en informatiebeveiliging naar de RvB.

Bijlage A: Goedgekeurde middelen (niet uitputtend)

Middelen
Telefoongesprek via werktelefoon
Werk email
SMS vanaf werktelefoon
KPN Zorg Messenger App
Videoconferencing (beveiligd)
LSP / Zorgnet
SURFfilesender
WhatsApp
Trello

Bijlage B: Niet goedgekeurde middelen (niet uitputtend)

Middel
Dropbox
WeTransfer
Facebook Messenger
FaceTime
Instagram
Privé e-mail
Privé telefoon
Signal
Skype / Skype for Business

Bijlage C: Doelstellingen competenties medewerkers

1. Je begrijpt dat we informatie moeten beschermen en kent de gevolgen als we dat niet doen.
2. Je gebruikt alleen goedgekeurde middelen voor je werk.
3. Je weet dat beperkt privégebruik van middelen is toegestaan zolang niemand er last van heeft en je je houdt aan de fatsoensnormen en de wet.
4. Je kent de gevoeligheidslabels (publiek, intern, vertrouwelijk en geheim) en weet wanneer je labels moet plaatsen.
5. Je kunt datalekken, phishing en andere informatiebeveiligingsincidenten herkennen, weet hoe te handelen en hoe je deze meldt.
6. Je begrijpt dat het ziekenhuis afhankelijk is van ICT en je oefent met de noodprocedures.
7. Je begrijpt het belang van fysieke beveiliging en je zorgt dat informatie ook fysiek veilig is.
8. Je begrijpt wat je moet doen om onze informatie en informatiesystemen veilig te houden en voorkomt incidenten.
9. Je beveiligt je thuiswerkplek.
10. Je wisselt gegevens veilig uit met collega’s, patiënten en anderen.
11. Je e-mailt en chat veilig.
12. Je internet veilig en houdt je aan de regels voor gratis online diensten.
13. Je videobelt veilig.
14. Je maakt veilig gebruik van je telefoon.

Gedragscode veilig gebruik van informatiemiddelen

15. Je maakt veilig gebruik van het EPD.
16. Je kent je eigen rol bij het veilig houden van informatie, de valkuilen daarbij en weet hoe je jezelf scherp kunt houden.
17. Je weet dat het ziekenhuis toezicht houdt op de informatievoorziening, dat er bij zwaarwegende redenen inzage kan zijn in jouw bestanden en informatie en ook dat er sancties kunnen volgen op overtredingen van het beleid.