GEDRAGSCODE INFORMATIEBEVEILIGING EN GEBRUIK ICT-FACILITEITEN ZIEKENHUISGROEP TWENTE

Deze gedragscode omschrijft het gebruik van alle informatie en ICT-faciliteiten ter beschikking gesteld door de Ziekenhuisgroep Twente (hierna: ZGT) aan haar eigen medewerkers, tijdelijk personeel, (vrijgevestigde) medisch specialisten en personeel dat door derden wordt ingezet (hierna: medewerkers) om diensten te verlenen aan onze organisatie en derden die van ZGT toestemming krijgen c.q. gevraagd zijn om onderzoek te doen en daarvoor ZGT informatie nodig hebben.

1. Overwegingen

De volgende punten zijn overwogen bij het vaststellen van deze gedragscode:

a. Gebruik van informatie en informatiesystemen is belangrijk voor ZGT om haar taken als ziekenhuis goed te kunnen vervullen. Echter, onjuiste omgang (bewust en onbewust verkeerd handelen) kost tijd, geld en capaciteit van mensen en apparatuur en brengt diverse risico's met zich mee.

b. Aan het gebruik van informatie en ICT-faciliteiten zijn, per verschijningsvorm, risico's verbonden die nopen tot het stellen van gedrags- en gebruiksregels. Bij risico's valt te denken aan:
   - oneigenlijke toegang tot (medische) informatie betreffende patiënten of ZGT informatie;
   - uitval van de ICT-systemen door cyberaanvallen, waaronder ransomware of andere virussen;
   - uitlekken van vertrouwelijke (patiënt)gegevens of bedrijfsgeheimen;
   - het in diskrediet brengen van de goede naam van het ziekenhuis.

c. Ter vermijding van dergelijke risico's geeft ZGT-voorschriften voor het verrichten van werkzaamheden met behulp van informatie en ICT-faciliteiten ter bevordering van de goede orde. De hierna in de hoofdstukken weergegeven regels vallen onder deze bepaling.

d. Tegen de achtergrond van de risico's van het gebruik van informatie en ICT-faciliteiten wordt van de gebruiker professioneel en integer handelen verwacht.

e. Het gebruik van applicaties, internet, e-mail, tokens, smartphones, telefoons, e.d. wordt vastgelegd. Deze registratie geschiedt om de continuïteit van de technische infrastructuur te waarborgen, om de verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan, en om toezicht te houden op de naleving van de gedrags- en gebruiksregels door de gebruiker.

f. Inhoudelijke controle van het internet-, e-mail- en computergebruik alsmede het gebruik van elektronische patiëntendossiers kan plaatsvinden indien sprake is van een vermoeden van in strijd handelen met de gedrags- en gebruiksregels door de gebruiker. Niet naleving van deze regels kan leiden tot disciplinaire maatregelen.

g. Deze gedragscode betreft:
   - De regels die de gebruikers moeten naleven bij het gebruiken van de door ZGT voor zakelijk gebruik ter beschikking gestelde informatie en (thuis-) werkplekken met applicaties, internet- en e-mailsystemen en telefoons;
   - De omstandigheden waaronder ZGT besluit tot het registreren, verzamelen, monitoren en controleren van tot personen herleidbare data

omtrent toegang tot (patiënt-)gegevens, internet-, e-mail-, computer- en telefoongebruik.

2. Doelstellingen

Met de gedragscode beoogt ZGT:

- Duidelijk te maken dat de ter beschikking gestelde informatie en ICT-faciliteiten in beginsel alleen bedoeld zijn als efficiënte hulpmiddelen bij het uitoefenen van werkzaamheden voor ZGT;
- Duidelijkheid te geven over de aard en wijze waarop van de informatie en ICT-faciliteiten gebruik mag worden gemaakt;
- De bewustwording te vergroten van het gebruik van informatie en de ICT-faciliteiten en de daaraan verbonden risico's;
- Negatieve gevolgen, zoals bijvoorbeeld het schaden van de privacy, binnenhalen van virussen of ongewenste publiciteit, voor ZGT te voorkomen.

3. Privacy

ZGT hecht aan de privacy van patiënten, medewerkers en medisch specialisten. Wet- en regelgeving staan toe dat ZGT controleert op onjuist gebruik dan wel misbruik van de bedoelde informatie en ICT-faciliteiten. Het streven hierbij is gericht op een goede balans tussen controle en privacybescherming.

4. Werkingssfeer

Deze gedragscode geldt voor eenieder die voor ZGT werkzaam is en/of die gebruik maakt van de informatie en ICT-faciliteiten van ZGT in verband met de uitoefening van diens functie.

De Raad van Bestuur eist dat deze gedragscode wordt nageleefd door iedereen waarop deze gedragscode van toepassing is.

5. Algemeen

De gebruikelijke gedragsregels, zoals de regels die momenteel gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van ZGT en voor het verzenden van post (zoals correct taalgebruik) zijn ook van toepassing op de ICT-infrastructuur.

6. Gebruik

6.1. Ten aanzien van het (elektronisch) patiëntendossier geldt het volgende:

- Bij de toegang tot (elektronische) patiëntendossiers mag de medewerker alleen gegevens inzien van een patiënt waarmee de medewerker een behandelrelatie heeft (of hierbij ondersteunt).
- Het is niet toegestaan patiëntendossiers te raadplegen voor andere doeleinden dan de werkzaamheden waarvoor de medewerker is aangesteld. Het uit nieuwsgierigheid raadplegen van een patiëntendossier van een bekende (bijvoorbeeld een bekende persoon, een buurvrouw of een collega die tevens patiënt is) is niet toegestaan.
- Voor patiënten is via het patiëntportaal inzichtelijk welke functionarissen (op functietitel) hun dossier hebben ingezien, ook daarom wordt van medewerkers voorzichtigheid verwacht.

6.2. Ten aanzien van het privégebruik geldt het volgende:

- Binnen ZGT mogen gebruikers van haar ICT-functionaliteiten naast zakelijk tevens beperkt persoonlijk gebruikmaken van deze voorzieningen. Gebruik is doorgaans verbonden met taken/bezigheden die voortvloeien uit de

functie. Daarbij dienen zij zich te houden aan de door ZGT opgestelde regels en procedures en voorts de daartoe door het ziekenhuis beschikbaar gestelde huisstijl te hanteren.
- Werknemers mogen ICT-faciliteiten incidenteel en kortstondig voor privédoeleinden gebruiken, zowel intern als extern, mits dit niet storend is voor de dagelijkse werkzaamheden en mits hierbij voldaan wordt aan de verdere richtlijnen van deze gedragscode.

6.3. Ten aanzien van het gebruik van de digitale werkplek geldt het volgende:
- Inlognaam, wachtwoord, pincode en/of toegangspassen zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven;
- Medewerkers dienen het wachtwoordbeleid van ZGT na te leven, hierbij hoort o.a. het hanteren van sterke wachtwoorden die niet overeenkomen met andere privéwachtwoorden en het niet onbeschermd opslaan/opschrijven van wachtwoorden in bestanden of op papieren;
- Inhoud en onderhoud van de persoonlijke home-directory (de aan de gebruiker ter beschikking gestelde digitale archiefruimte) valt volledig onder de verantwoordelijkheid van de gebruiker zelf;
- Het up- en downloaden van software/applicaties en films is niet toegestaan (tenzij een uitzondering geldt voor medische toepassingen);
- Vertrouwelijke gegevens, daaronder altijd alle patiënt- of medewerkersgegevens begrepen, en bedrijfsgevoelige informatie mogen nimmer zonder wettelijke grondslag of zonder expliciete toestemming van de betrokkene(-n) naar buiten de organisatie worden verstuurd.
- Bij verzending/uitwisseling van informatie (zowel intern als extern) dient de medewerker alleen de goedgekeurde communicatiekanalen te gebruiken zoals gesteld in het beleid informatietransport;
- Indien men de werkplek verlaat dient men het systeem te vergrendelen, uit te loggen of uit te schakelen (clear screen);
- Het is niet toegestaan inkomende privé-berichten te genereren door deel te nemen aan nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke.

6.4. Ten aanzien van het gebruik van de fysieke werkplek geldt het volgende:
- Sluit onbewaakte kamers/ruimtes af om ongeautoriseerde toegang tot de hierin aanwezige apparatuur, papieren, e.d. te voorkomen.
- Laat kamers en bureaus schoon en opgeruimd achter, sluit bureaus en kasten af en berg de sleutels veilig op.
- Berg papieren dossiers, waardevolle voorwerpen en draagbare apparatuur achter slot en grendel op (clean desk);
- Er dient geen vertrouwelijke informatie achter te blijven op computers (waaronder beeldschermen), printers of papieren waar iedereen gemakkelijk bij kan.

6.5. Ten aanzien van het gebruik van internet is het niet toegestaan om:
- Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- Pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden;
- Zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet;
- Opzettelijk informatie waartoe men via internet toegang heeft verkregen zonder toestemming te veranderen of te vernietigen.

Indien een medewerker of gebruiker ongevraagd informatie van deze aard krijgt aangeboden, dient deze dat aan de servicedesk (3333) dan wel zijn leidinggevende te melden.

ZGT behoudt zich het recht voor om de toegang tot bepaalde internetsites te beperken. Vanuit de in de vakliteratuur benoemde risico's blokkeert de afdeling ICT websites die risico's opleveren uit beveiligingsoogpunt. ZGT kan het recht tot gebruik van (een deel van) internet toestaan, maar ook altijd weer intrekken. Zonder dat recht, is gebruik van (een deel van) internet niet toegestaan.

6.6. Ten aanzien van social media geldt het volgende:
- Bestuurders, managers, leidinggevenden en degene die namens de organisatie het beleid en de strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik maken van social media. Voor sommige functies geldt dat iemand altijd wordt gezien als ZGT-er – ook als hij een privémening verkondigt. Op grond van hun positie moeten werknemers nagaan of zij op persoonlijke titel kunnen publiceren.
- Medewerkers mogen geen informatie verstrekken over patiënten, bezoekers, collega's, etc.
- Medewerkers mogen geen video's, foto's of andere informatie delen waarvan men redelijkerwijs kan vermoeden dat hiermee gevoelige of vertrouwelijke (bedrijfs)informatie prijs wordt gegeven.
- Bij de geringste twijfel over raakvlakken met ZGT is het verstandig contact te zoeken met de leidinggevende.
- Zie KIS-document 'Social media, gedragscode'.

6.7. Ten aanzien van e-mail is het niet toegestaan om:
- Berichten anoniem of onder een fictieve naam te versturen;
- Dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailberichten te verzenden of door te sturen;
- Iemand elektronisch lastig te vallen.

Indien een medewerker of gebruiker ongevraagd informatie van deze aard aangeboden krijgt, dient deze dit te melden aan de servicedesk (3333) dan wel zijn leidinggevende.

6.8. Ten aanzien van het gebruik van de (mobiele) ZGT telefoon geldt het volgende:
- Medewerkers mogen telefoons van ZGT gebruiken in het kader van hun functie-uitoefening;
- Incidenteel en kortstondig gebruik van de telefoon voor het voeren van privégesprekken is toegestaan, mits dit geen storende onderbreking vormt van de werkzaamheden en mits dit niet storend is voor het telefoonnetwerk;
- Voor medewerkers die een mobiel toestel van ZGT in gebruik hebben, geldt bovendien dat zij zich houden aan de regels die door ZGT omtrent het gebruik van mobiele telefoons zijn vastgelegd;
- Het is niet toegestaan om door ZGT verstrekte telefoonaansluitingen te gebruiken om:
  - Service- en amusementsnummers te bellen;
  - Internationale nummers te bellen voor privédoeleinden;
  - Rechtstreeks in te bellen op een ISP-toegangsnummer (Internet Service Provider), tenzij hiervoor vooraf schriftelijk toestemming is verleend;
  - Anderszins ongeoorloofde handelingen in dit verband te verrichten.

Oneigenlijk gebruik van telefoons kan een verstoring van de werkzaamheden of een verstoring van het telefoonnetwerk veroorzaken en bovendien tot financiële schade voor ZGT leiden.

6.9. Ten aanzien van het gebruik van een mobiele ZGT-werkplek (buiten ZGT-muren via een laptop, telefoon, tablet, o.i.d) geldt:
- Medewerkers moeten zich houden aan de regels die door ZGT omtrent het gebruik van de mobiele werkplek zijn vastgesteld, waaronder het beleid structureel thuiswerken;
- Medewerkers moeten bij het werken via een mobiel apparaat (met name in geval van een privéapparaat) veilig en professioneel handelen i.r.t. de informatiebeveiliging, hierbij hoort o.a. dat:
  - alleen gebruik wordt gemaakt van vertrouwde wifi-verbindingen;
  - het apparaat is voorzien van antivirus tooling, qua beveiligingsupdates nog wordt ondersteund en tijdig geüpdatet is;
  - voorzichtig wordt gewerkt in openbare plekken t.a.v. het meekijken met of het meeluisteren van werk-gerelateerde zaken;
  - werk-gerelateerde informatie alléén binnen de door ZGT aangeboden en beheerde ICT-systemen opgeslagen wordt en geen (vertrouwelijke) ZGT-informatie lokaal op het apparaat opgeslagen is.
- Bij het verlaten van de mobiele ZGT-werkplek, dient het scherm te worden vergrendeld of uit te worden gelogd.

6.10. Het is ook anderszins niet toegestaan om met behulp van de door ZGT ter beschikking gestelde informatie en ICT-faciliteiten in strijd met de wet of onethisch te handelen.

6.11. Social engineering en/of identiteitsdiefstal
Pas op voor buitenstaanders die proberen toegang te krijgen tot vertrouwelijke gegevens of computersystemen. Dit door zich voor te doen als bijvoorbeeld een technicus van een bedrijf en dan naar wachtwoorden en gebruikersnamen te vragen. Verstrek nooit vertrouwelijke informatie zoals patiëntgegevens, inlognamen of wachtwoorden aan iemand wiens identiteit u niet kan controleren.

Wees tevens bedachtzaam op andere dreigingen zoals phishing-mails (met name links of bestanden in e-mails) of verzoeken tot het aanpassen van bankrekeningnummers of overmaken van geld.

6.12. Melden van incidenten met betrekking tot informatiebeveiliging
- Onbedoelde inbreuken op de beveiliging, zoals het kwijtraken van (mobiele) apparatuur en uitlekken van (inlog)gegevens, dienen aan de servicedesk (3333 of servicedeskICT@zgt.nl) te worden gemeld;
- Indien persoonsgegevens uitlekken, dan treedt ook het protocol melden datalekken in werking t.b.v. beoordeling en afhandeling.

7. Controle

7.1. Regelmatig en steekproefsgewijs zullen controles plaatsvinden ten aanzien van het gebruik van elektronische patiëntendossiers. Hierbij zal de nodige zorgvuldigheid worden betracht om de privacy van de gebruiker te beschermen.

7.2. Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik overeenkomstig deze regeling, worden van tijd tot tijd controles uitgevoerd. Hiernaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Dit geldt eveneens voor telefonie-voorzieningen.

7.3. Binnenkomend en uitgaand internet- en e-mailverkeer (inclusief bijlagen) wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Mocht blijken dat een e-mailbericht een virus en/of potentieel risicovolle bestanden bevat, dan wordt het automatisch tegengehouden. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met de servicedesk (3333).

7.4. Het internet- of e-mailverkeer zal anders dan door de virusscanner zelf, in geen geval buiten situaties van acute overmacht, door het ziekenhuis worden geopend. Een uitzondering hierop vormen situaties als bedoeld hierna onder 7.6 waarbij sprake is van een redelijke verdenking of een vermoeden van ongeoorloofd handelen.

7.5. Ingeval internet- of e-mailverkeer geopend moet worden in een situatie van acute overmacht als hiervoor onder 7.4 bedoeld, wordt hiervan een "calamiteitenverslag" opgemaakt welk terstond wordt overgelegd aan de betrokkene(-n).

7.6. Indien mocht blijken dat in strijd met deze regeling wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten de organisatie en systeemstoringen), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt. Controleren alsmede openen van e-mail, ook die voor privégebruik, ten behoeve van het opsporen van onrechtmatig gedrag van de werknemer dan wel de gebruiker is dus toegestaan indien er sprake is van een redelijke verdenking of een vermoeden van ongeoorloofd handelen.

7.7. De betreffende gegevens worden bewaard zolang dit in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is.

7.8. Alle bij het interne- en/of e-mailverkeer betrokken (ICT-)medewerkers hebben de plicht tot volledige geheimhouding over al datgene wat zij in hun werk ten aanzien van het internet en e-mailgebruik in het ziekenhuis vernemen.

8. Maatregelen

Bij handelen in strijd met deze regeling, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van de ter beschikking gestelde ICT-faciliteiten, kunnen afhankelijk van de aard en de ernst van de overtreding (disciplinaire) maatregelen worden getroffen conform het 'sanctioneringsbeleid van ZGT'. Hierbij moet worden opgemerkt, dat indien een werknemer zich schuldig maakt aan bijvoorbeeld het raadplegen van patiëntinformatie van patiënten waar geen behandelrelatie mee bestaat, het bezoeken van pornosites en het verzenden van e-mailberichten met pornografische afbeeldingen, arbeidsrechtelijke consequenties kunnen volgen en zelfs, onder omstandigheden, ontslag op staande voet kan volgen, dan wel ontbinding van de arbeidsovereenkomst c.q. toelatingsovereenkomst zal worden verzocht aan de kantonrechter c.q. Scheidsgerecht.

9. Slot

In alle gevallen waarin deze regeling niet voorziet, beslist de Raad van Bestuur.