Protocol Elektronisch communicatieverkeer + informatievoorzieningen



Zorgvuldig omgaan met informatie en het delen daarvan

Informatie delen doe je dagelijks. In een gesprek, op papier, via e-mail, social media, WhatsApp of andere media. Zorgvuldig omgaan met het delen van informatie is in je werk essentieel. Die informatie gaat vaak direct of indirect over onze cliënten; mensen waarmee wij een vertrouwensrelatie hebben.
Dit protocol geeft handvatten hoe je zo veilig mogelijk met het delen van werk-gerelateerde informatie kunt omgaan.

Als professional ga je respectvol om met (privacy) gevoelige informatie - zie ook het Protocol Privacy. Wees je bewust welke informatie je via welke weg gaat delen en bespreek dit eventueel met je collega's. Gebruik waar mogelijk de digitale communicatiemiddelen die via het Philadelphia systeem beschikbaar zijn om (privacy) gevoelige informatie te delen.

Hoe pak je dit aan?

1. Bespreek met je collega's hoe je veilig informatie kan en wilt delen.
2. Vergrendel je apparatuur als je (even) weggaat en houd je inlognaam en wachtwoord voor jezelf.
3. Zorg dat je gevoelige informatie, als je jouw werkplek verlaat, in een af te sluiten kast bewaard.
4. Bespreek met je leidinggevende als je vertrouwelijke informatie wilt delen met externen. Als je cliënt-informatie wilt delen met externen bespreek dit met de cliënt/vertegenwoordiger. Deel cliënt-informatie via ShareFile en/of de app Citrix Files.
5. Wanneer je op diverse werkplekken of thuis werkt, ga dan zorgvuldig om met het meenemen van informatie.
6. Bezoek, download of verspreid geen informatie die racistisch, discriminerend, pornografisch, beledigend of aanstootgevend is.
7. Wees voorzichtig met het openen van e-mails van verdachte afzenders en vooral met het openen van bestanden die je niet verwacht.
8. Gedraagt de computer, smartphone e.d. zich anders dan anders, neem dan contact op met de Servicedesk ICT.
9. Gebruik van communicatiemiddelen voor privé doeleinden tijdens je werk is beperkt toegestaan zolang het de kwaliteit en productiviteit van je werk niet negatief beïnvloedt.
10. Meld alle voorvallen waar je denkt dat er (per ongeluk) onverantwoord met informatie is omgegaan of gegevens in verkeerde handen is terecht gekomen, bij de Servicedesk ICT. Dan kunnen we op tijd maatregelen treffen om erger te voorkomen.

"Als collega's stuurden we wel eens vertrouwelijke documenten naar elkaars privé e-mailadres om er 's avonds thuis aan te kunnen werken. We hebben geregeld dat we ook thuis in kunnen loggen op het netwerk van Philadelphia, dan blijven de documenten binnen de digitale werkomgeving"

Facts & Figures

Wie heeft een taak?
- Alle medewerkers, leerlingen, stagiaires, uitzendkrachten, vrijwilligers, extern ingehuurden
- Leidinggevenden
- Security functionaris van het cluster
- Afdeling I&A
- Privacy Officer
- Security Officer

Status
Dit protocol berust op de Algemene Verordening Gegevensbescherming (AVG) en de norm ISO27001.

Document eigenaar
Directeur Medewerkersbelang

Voor het laatst aangepast
Juni 2023

Evaluatietermijn
Iedere twee jaar

Gerelateerde documenten
- Juridische bepalingen (bijlage)
- Handreiking Sociale Media
- Protocol Privacy
- Gedragscode
- Protocol Huisregels
- Protocol Veiligheid
- Protocol Ongewenste gebeurtenissen

Welke middelen?
Dit protocol gaat over het delen van informatie met specifieke aandacht voor diverse platforms en middelen zoals: internet, Mijn Philadelphia, e-mail, social media, laptop, smartphone, iPad.

Social media
Deze media zijn laagdrempeling; een bericht is zo geplaatst. Besef dat jouw berichten door veel mensen gelezen kunnen worden. Zie ook de handreiking Social Media.

Servicedesk

servicedesk.ict@philadelphia.nl
of 033 - 760 22 22

Voor vragen over elektronisch communicatieverkeer.



"Je mag natuurlijk best tijdens een verjaardagsfeestje vertellen dat je een drukke dag hebt gehad op de locatie. Maar ga niet vertellen dat cliënt Jan Schilder vandaag alweer een woede-uitbarsting heeft gehad en het meubilair in zijn kamer kapot heeft gemaakt. En laat niet op de tuintafel het cliëntdossier op je iPad openstaan terwijl je even bij de buren een kop thee drinkt."

Wist je dat? En tips

Beveiliging digitale diensten
Philadelphia beveiligt haar digitale omgeving om zorgvuldig met (privacy) gevoelige informatie om te gaan. Denk hierbij aan gevoelige informatie rondom cliënten, medewerkers en organisatie. Deze beveiliging is ook nodig om te voldoen aan wetgeving op dit gebied.

Gevoelige informatie
Als je (privacy) gevoelige informatie wilt delen doe dit dan mondeling of gebruik de Philadelphia digitale diensten om te communiceren. Voor het veilig delen van informatie (met externen) kun je gebruik maken van Sharefile, iedere medewerker heeft toegang tot Sharefile via PhilaNet → .
Om foto's en/of films te delen kun je de app Citrix Files gebruiken.
Gebruik de juiste systemen (ECD, Youforce, InPlanning etc.) en bespreek met je collega's wanneer je wat gebruikt.

Algemeen nieuws
Philadelphia gebruikt het internet, Facebook en Twitter e.d. voor algemeen nieuws dat met iedereen gedeeld mag worden.

DigiContact
De medewerkers van DigiContact maken contact met een cliënt via beeldcommunicatie via een beveiligde, digitale omgeving. Skype is hiervoor ongeschikt.

Skype, Facetime, Facebook, Instagram, Whatsapp, Dropbox, Prezi e.d.
Deze diensten zijn niet gericht op veilige communicatie en slaan gegevens op hun servers (vaak in het buitenland) op. Daarmee zijn ze ongeschikt voor het delen van privacy gevoelige informatie. Maak je een presentatie in de gratis versie van Prezi, bedenk dan dat deze presentatie voor iedereen (in- en extern) is in te zien.

Online vergaderen en beeldbellen
Voor online vergaderen gebruiken we Webex. Daarnaast is Jabber beschikbaar voor beeldbellen. Via deze systemen kun je veilig online vergaderen of beeldbellen. Meer informatie vind je op PhilaNet.





Controle

Wanneer Philadelphia het vermoeden heeft dat je in strijd met dit protocol handelt, dan heeft zij het recht om jouw gebruik van de diverse informatievoorzieningen te controleren. Je wordt wel van tevoren geïnformeerd over het doel van de controle en welke gegevens gecontroleerd worden. Afhankelijk van de ernst van het vermoeden kun je hangende het onderzoek geschorst of op non-actief gesteld worden.
Wanneer blijkt dat je in strijd met het protocol handelt kan Philadelphia arbeidsrechtelijke maatregelen treffen zoals: een officiële waarschuwing, een overplaatsing of ontslag (op staande voet). Dit zal afhankelijk zijn van de aard en de omvang van het handelen. Zie ook de **bijlage** met juridisch bepalingen behorende bij dit protocol.

1008PROT_027

Heb je nog vragen en/of opmerkingven?
Mail ons