Bijlage 6

Classificatie van beveiligingsrisico's

Dit document zorgt voor grotere bewustwording in de gehele organisatie door te benoemen en te registreren welke informatie als vertrouwelijk, intern of openbaar wordt beschouwd. Ook biedt het aanknopingspunten voor de discussie over thuiswerken. Daarnaast vindt u hierin enkele richtlijnen voor het opstellen van formats voor memo's, documenten, notulen en het gebruik van predikaten als 'vertrouwelijk', 'intern' en 'openbaar'.

1. Doelstelling

Classificatie van bedrijfsprocessen, informatiesystemen en informatie levert een bijdrage aan de beveiliging van deze bedrijfsprocessen, informatiesystemen en informatie. Op basis van de classificatie van deze objecten kunnen prioriteiten voor beveiliging worden gesteld, 'beveiliging op maat' dus. Daarom wordt binnen de CIHN bijvoorbeeld gebruik gemaakt van een classificatiesysteem. Dit stelt ons in staat de verschillende beveiligingsniveaus te definiëren en per klasse specifieke minimumregels te stellen voor de beveiliging van bedrijfsprocessen, informatiesystemen en informatie.

2. Doelgroep

Bureau organisatie van de CIHN alsmede locatiemanagers, CODA's en teamleider Nijmegen.

3. Afkortingen

CODA	Coördinerend doktersassistente
EPD	Elektronisch Patiënten Dossier
ALV	Algemene Ledenvergadering
DA	Doktersassistenten
HA	Huisartsen

4. Werkwijze

4.1 Inleiding

De CIHN behoeft een passend classificatiesysteem voor informatie (documenten, registraties, presentaties, etc.), gegevens (EPD en/of delen daaruit) en fysieke locaties (toegang).
Volgens de NEN 7511-2 norm is het noodzakelijk vast te leggen welke maatregelen horen bij welke classificatie en dit periodiek te evalueren. Om beveiligingseisen te kunnen opstellen moeten gegevens geclassificeerd worden.

4.1.1 Risicoanalyse en middelenmatrix

Voor het classificeren van fysieke locaties, registraties, bewaarplaatsen en dergelijke is gekozen voor de indeling van beschikbaarheid, integriteit en vertrouwelijkheid.
Hierbij kan gekozen worden voor de klassen Hoog, Midden en Laag (zie volgende paragraaf voor toelichting).

De classificatie van de systemen, bestanden en fysieke locaties die voor de CIHN relevant zijn, is vastgelegd in het document over risicoanalyses en het document met de middelenmatrix (zie bijlage 5 en 10).

4.1.2 Indeling beschikbaarheid

Voor de beschikbaarheid van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Beschikbaarheid	
Klasse	**Definitie**	**Voorbeeld**
Laag	Uitval van het bedrijfsproces, informatie(systeem) levert geen schade op voor de CIHN	Voorlichtingsactiviteiten
Midden	Uitval van het bedrijfsproces, informatie(systeem) levert beperkte schade op voor de CIHN	Financiële administratie
Hoog	Uitval van het bedrijfsproces, informatie(systeem) levert grote schade op voor de CIHN	Patiëntenregistratie

4.1.3 Indeling integriteit

Voor de integriteit van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Integriteit	
Klasse	**Definitie**	**Voorbeeld**
Laag	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatie(systeem) levert geen schade op voor de CIHN	
Midden	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatie(systeem) levert beperkte schade op voor de CIHN	Verslag werkoverleg
Hoog	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatie(systeem) levert grote schade op voor de CIHN	Elektronisch Patiënten Dossier

4.1.4 Indeling vertrouwelijkheid

Voor de vertrouwelijkheid van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Vertrouwelijkheid	
Klasse	**Definitie**	**Voorbeeld**
Laag 'Openbaar'	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatie (systeem) levert geen schade op voor de CIHN	Patiëntenbrochure
Midden 'Voor intern gebruik'	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatie(systeem) levert beperkte schade op voor de CIHN	Projectadministratie
Hoog 'Vertrouwelijk'	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatie(systeem) levert grote schade op voor de CIHN	Patiëntendatabase

Dit document betreft met name de vertrouwelijkheid van documenten en bestanden.

4.2 Classificatie van documenten

4.2.1 Waarom classificeren van documenten?

Binnen de CIHN worden veel documenten opgesteld en rondgestuurd aan de verschillende betrokkenen. Hierbij is het van groot belang dat medewerkers zich bewust zijn van de gevoeligheid van de informatie die zij krijgen, dan wel verstrekken.
Door het classificeren van informatie en documenten wordt voorkomen dat onbedoeld informatie buiten de CIHN terecht komt die daar niet hoort te zijn.
Uitzonderingen worden door de directie bepaald.

Om incidenten te voorkomen zijn afspraken gemaakt over de classificatie van documenten en informatie. Als hulpmiddel hebben we hiervoor een format voor memo's en notulen ontwikkeld en geïmplementeerd.
Dit format vraagt om de volgende informatie:
Betreft/Datum/Auteur/Van/Aan of Doelgroep/Aanwezigen/Status/Classificatie en Documentnummer.
(zie voorbeeld onderaan dit document).

4.2.2 Doelgroepen

De volgende (interne) doelgroepen zijn te onderscheiden:

- Bestuur;
- ALV (afgevaardigden van alle leden);
- HA (alle huisartsen, is nog intern);
- DA (alle doktersassistenten, is nog intern);
- MT-leden;
- Medewerkers uit bureauorganisatie ("kantoor").

Daarnaast kennen we patiënten, het algemene publiek (inwoners van het verzorgingsgebied) en externe relaties. Met name bij externe relaties en bij patiënten kan soms ook sprake zijn van vertrouwelijke informatie.

4.2.3 Afspraken over classificatie

De volgende afspraken zijn gemaakt:

- Alle stukken die geschreven worden binnen de CIHN zijn in principe 'intern', tenzij anders bepaald.
- Alle stukken die nog in concept zijn, zijn altijd intern.
- Patiëntgegevens zijn altijd vertrouwelijk.
- Bestuursnotulen en aanverwante stukken zijn altijd vertrouwelijk.
- Personeelsgegevens zijn vertrouwelijk.
- Formats voor de invoer van prestatie-indicatoren of begroting zijn intern.
- Ingevulde formats met prestatie-indicatoren en financiële gegevens zijn vertrouwelijk.
- Patiëntgegevens zijn daarnaast zodanig vertrouwelijk dat zij niet per mail mogen worden verstuurd, ook niet binnen de organisatie.
- Patiëntgegevens verlaten nimmer het pand, tenzij dit een onderdeel is van het werkproces (dus wel voor het rijden van visites; niet voor het thuiswerken aan klachten).
- Gevoelige personeelsgegevens worden waar mogelijk geanonimiseerd alvorens te mailen.
- Alle zaken rondom klachten zijn vertrouwelijk. Hierover wordt alleen gesproken met betrokkenen, die daarover naar buiten toe niets mededelen.
- Bij vertrouwelijke documenten wordt expliciet de naam genoemd van degenen die het stuk ontvangen (dus niet aan “het bestuur”, maar de namen van de personen).
- Alle intern-geclassificeerde stukken zijn alleen bedoeld voor de doelgroep en mogen niet verder worden verspreid.
- Alle stukken in het kwaliteitshandboek zijn intern, tenzij anders geclassificeerd (enkele documenten verdienen de status vertrouwelijk). De documenten worden alle voorzien van een classificatie (intern/vertrouwelijk).
- Het openbare deel van de website (voor patiënten) is openbaar; hetzelfde geldt voor definitieve jaarverslagen en kwaliteitsjaarverslagen.
- Het gesloten deel van de website is beschikbaar voor medewerkers, dan wel huisartsen. Hierop zijn interne documenten te vinden die alleen na toestemming van de directeur openbaar kunnen worden gemaakt.
- Na inloggen met een UZI-pas is alle informatie vertrouwelijk (patiëntinformatie). Houd hiermee rekening bij het laten meekijken (bewust of onbewust) op je scherm.
- Bij het mailen van vertrouwelijke of interne informatie is het wenselijk vooraf te rade te gaan bij de personen aan wie u de informatie richt. Waar nodig kan ook al in de mail aan de geadresseerden vermeld staan dat het aangehechte document vertrouwelijk is (ook als dit al op het document staat beschreven).
- Bestanden van buitenaf (presentaties, et cetera) worden niet geclassificeerd, tenzij deze ook gevoelige informatie over de eigen organisatie bevatten. Het is aan de afzender een classificatie aan te geven (bijvoorbeeld: intern, concept, onder embargo, et cetera).

Medewerkers dienen op de hoogte te zijn van de classificatie en zich te houden aan de hier beschreven regels. Afwijking van de afgesproken hiervan classificatie (bijvoorbeeld het laten lezen van klachtbrieven aan medewerkers die niet bij de afhandeling zijn betrokken, het versturen van bestuursnotulen aan de ALV) wordt gezien als een beveiligingsincident. Dit dient gemeld te worden bij de leidinggevende die dit registreert en communiceert met de kwaliteitsfunctionaris. In ernstige gevallen (waarbij direct handelen gewenst is) wordt de directeur erbij betrokken.

4.3 Thuiswerken van kantoormedewerkers met interne of vertrouwelijke documenten

Diverse medewerkers werken thuis. Dit gebeurt momenteel deels met webmail, deels met laptops van de organisatie. Met de laptops is (via VPN) toegang tot de archivering. Dit voorkomt dat documenten lokaal worden opgeslagen. Via webmail kunnen documenten worden gemaild om thuis te gebruiken. Deze documenten worden dan wel lokaal opgeslagen.

4.3.1 Risicoanalyse thuiswerken met documenten/bestanden

De risico's zijn in kaart gebracht op volgorde van hoog naar laag.

Toepassing	Risico klasse	Omschrijving	Oplossing
Documenten mailen naar privé-email	Zeer hoog	Door het mailen naar ongecontroleerde privé-accounts komen gegevens in een volledig onbeschermde omgeving. Er is geen garantie dat er een virusscanner actief is en dat het e-mailaccount niet door meerdere personen gelijktijdig gebruikt wordt.	Inzet van laptops van de organisatie Het gebruik van webmail dan wel VPN- verbinding
Lokaal opslaan van bestanden	Hoog	Het lokaal opslaan van bestanden op niet beveiligde pc. Deze gegevens kunnen onbedoeld op straat komen te liggen door inbraak, mede pc-gebruikers, diefstal/inbraak of virussen/hackers.	Inzet van laptops van de organisatie <u>Alternatief:</u> Vertrouwelijke documenten niet lokaal opslaan, interne documenten z.s.m. verwijderen
Meekijken door derden	Hoog	Meekijken door derden op scherm, in bestanden of op papier.	Verantwoordelijkheid van de betreffende functionaris. Door training en bewustwording risico beperken
Gebruik organisatie laptop met UMTS-verbinding dan wel VPN-verbinding op eigen pc	Laag	Veilig t.a.v. hacken, diefstal pc, lokaal opslaan, toegang door gezinsleden. Meekijken blijft wel een risico.	Eigen verantwoordelijk-heid medewerker

In volgorde van onveilig naar veilig:

a. thuiswerken via documenten in de privémail (documenten worden dan ook lokaal opgeslagen);
b. thuiswerken via documenten in de webmail (wel lokaal documenten opslaan);

c. thuiswerken via VPN-verbinding, waardoor de medewerker bij de archiveringsbestanden kan. Speciale vereisten zijn nodig voor de instelling van de thuiscomputer;
d. thuiswerken via een laptop of desktop met UMTS-verbinding en VPN.

4.3.2 Regels die in acht genomen moeten worden bij het thuiswerken

- Geen werkdocumenten versturen naar het privé-mailadres; gebruik van in ieder geval webmail.
- Vertrouwelijke documenten mogen alleen via VPN geopend worden en niet lokaal worden opgeslagen.
- Documenten die lokaal worden opgeslagen, moeten zo snel mogelijk weer verwijderd worden.
- Gedrag: niemand mee laten kijken met de documenten; aantekeningen op papier niet rond laten slingeren.
- Bij voorkeur gebruikmaken van een organisatie-laptop (als de medewerker daarover beschikt).
- Alleen gebruikmaken van toegang tot patiëntenregistratie als het niet anders kan. (alleen mogelijk voor bereikbaarheidsdienst bij calamiteiten t.a.v. continuïteit van de dienstverlening).
- Afhankelijk van de individuele werkzaamheden die thuis gedaan moeten kunnen worden, kiezen voor een VPN-verbinding, dan wel gebruikmaken van een laptop/desktop met UMTS-verbinding voor de MT-leden.
- Kantoormedewerkers in het bezit van UZI-pas of Digipas dienen hun passen op de CHN achter te laten (m.u.v. bereikbaarheidsdienst).

Zorg dat alle medewerkers op de hoogte zijn van deze regels.

Format memo's / notulen

Betreft:	Onderwerp
Datum:	Datum
Opsteller:	Naam
Aan / doelgroep:	Bijv. locatiemanagers
Aanwezigen:	Indien van toepassing
Status:	Concept / Definitief / Vastgesteld door:
Classificatie:	Intern / Openbaar / Vertrouwelijk
Documentnummer	yyyymmdd, titel, initialen, versie nummer

Als voettekst wordt aangehouden:

Titel Pagina 7 van 7 datum: 14-12-2009

Linksonder: Titel
Midden: paginanummering
Rechts: Datum