UMCNL Standaard

Dataclassificatie en -labelling

Onderdeel van Data Governance voor Umc's
Datum: 18 juli 2025
Versie: 1.0

Voorwoord

Informatieveiligheid en digitale weerbaarheid is binnen de Umc's van groot belang. Om de dataclassificatie en het labellen van ongestructureerde data op een vergelijkbare wijze door de Umc's te kunnen uitvoeren is deze Nederlandse Federatie van Universitair medisch centra (NFU) standaard opgesteld door een grote groep experts die de Umc's vertegenwoordigen.

De standaard die hier voor u ligt is een levend document, waarvan wij geloven dat dit het begin is van een bredere samenwerking tussen de Umc's, waaronder in het data governance en het datamanagement werkgebied. We beoogden de handen ineen te krijgen om gezamenlijk de kennis, tijd en ervaring te delen om zo de Umc's algeheel rijker te maken en verder vooruit te helpen. Wij hopen, eveneens als eerdere projecten in het verleden, bijgedragen te hebben aan een samenwerkingsdrive die vanaf dit moment verder ontluikt.

Deze standaard is een samenwerking ontstaan vanuit de NFU en Ellen van Meurs (Microsoft). De projectgroep "DaGo" bestaande uit Arnold Kempenaar, Dennis Richel, Sander Vols en Ellen van Meurs, heeft de lijnen uitgezet voor de totstandkoming van dit document. Onder leiding van de projectgroep en Sacha Rütten is het document met de volgende schrijvers tot stand gekomen: Kerem Küçük, Kim Kortis, Martijn van Marle, Mitchell Howell, Nico Poppelier, Paul Leeraert, Rob den Bieman, Sebas van Hemert, Marc Blok, Sylvia Vogelaar, Ymkje Koster-Reidsma.

Daarnaast willen we de workshop deelnemers bedanken voor hun input gezien dit het fundament voor de inhoud van het document is geweest: Aychelin Ruschmeyer, Belinda de Bruijn, Ben Booij, Birgit Wouters, Chris Pothast, Guus Martens, Han Boter, Kerem Küçük, Kim Kortis, Koen Paulissen, Marieke Groeneveld, Marjoke Neut, Martijn van Marle, Nico Poppelier, Michel Dieben, Mitchell Howell, Paul Broertjes, Paul Leeraert, Odett Kieviet, Raoul Boomsma, Richard de Vet, Rik Jacobs, Ronald Bark, Rob den Bieman, Ruben Bremen, Sander van den Heuvel, Sebas van Hemert, Sylvester Muts, Sylvia Vogelaar, Tom Delnoy, is dit document gerealiseerd.

Al deze personen hebben stuk voor stuk het document naar een grotere hoogte gebracht. Mede dankzij de sponsoring van Frank Beckers, Jeroen van Rooden, Paulus Wieringa, Paul Grimberg, Sander Vols en de SIG-IB, de SIG-Architectuur, de Taczie en de Aczie heeft het project groen licht gezien.

Samenvatting

In een wereld die steeds verder digitaliseert, wordt het beheer van data een kritieke factor voor organisaties, waaronder de Universitair Medische Centra (Umc's) in Nederland. De Umc's van Nederland hebben zich middels de gremia Aczie, Taczie, SIG-IB, Sig-Architectuur gecommitteerd aan een gestandaardiseerde aanpak voor data governance, met als hoofddoel het optimaliseren van ongestructureerd datagebruik, terwijl de risico's worden geminimaliseerd en aan wet- en regelgeving wordt voldaan.

In dit document wordt voor in een uniforme aanpak van informatiemanagement een raamwerk voor dataclassificatie en labelling gepresenteerd, dat gericht is op het optimaliseren van het gebruik van ongestructureerde data binnen de Umc's van Nederland. Met het oog op de aanwezige gegevens binnen de Umc's, het belang van de bescherming ervan en het vertrouwen van patiënten is deze standaard opgezet.

Dit raamwerk biedt een gestandaardiseerde aanpak voor het bereiken van de volgende doelstellingen; de bescherming en het optimaliseren van de lifecycle management van ongestructureerde gegevens, naleving van wet- en regelgeving, verbetering van samenwerking tussen de Umc's, efficiëntie, en het vergroten van het vertrouwen van patiënten.

Om deze doelstellingen te bereiken dienen de Umc's de standaard op te nemen als onderdeel van de dagelijkse werkzaamheden en tot implementatie over te gaan. Verschillende stappen dienen hiervoor in acht te worden genomen, waaronder training en bewustwording, monitoring en samenwerking.
Door deze doelstellingen en acties na te streven, willen de Umc's van Nederland een robuust, uniform en effectief raamwerk opzetten. Dit raamwerk dient als basis voor samenwerking, efficiëntie en innovatie in de medische sector, het onderwijs en in het onderzoeksveld.

1. Inleiding

Dataclassificatie is een onderwerp dat op zichzelf erg breed is en moet worden gezien in een bredere context van data governance. De context en condities waarmee dataclassificatie is uitgewerkt voor deze industriestandaard is in dit hoofdstuk uiteengezet.

1.1 Dataclassificatie in de context van data governance

Data governance is het geheel van beleidsregels, procedures, rollen en verantwoordelijkheden die organisaties implementeren om de kwaliteit, beveiliging, beschikbaarheid en integriteit van data gedurende de gehele levenscyclus te waarborgen. Het doel van data governance is ervoor te zorgen dat data accuraat, consistent en compliant is met zowel interne als externe regelgeving, zodat deze effectief kan worden ingezet binnen en buiten bedrijfsprocessen.

Belangrijke onderwerpen binnen data governance zijn onder andere:

- Databewustzijn – Het besef van het belang, de juiste omgang en de beveiliging van data.
- Datakwaliteit – De waarborging van nauwkeurige, consistente en actuele data.
- Document- en contentmanagement – Het beheer van ongestructureerde data, zoals documenten en media.
- Metadata-management – Het beheer van gegevens over data, zoals definities, herkomst en relaties.`
- Data-privacy en beveiliging – De bescherming van gevoelige gegevens en naleving van relevante wetgeving.
- Data-compliance en bijbehorende regelgeving – Het voldoen aan interne en externe richtlijnen en wet- en regelgeving.
- Data-integratie – Het samenbrengen en synchroniseren van data uit verschillende systemen en bronnen.
- Data-lifecycle management – Het beheer van data gedurende de gehele levenscyclus, van creatie tot archivering of verwijdering.
- Data-auditing en -monitoring – De controle en het toezicht op datakwaliteit, -toegang en -gebruik.

Uitgebreide definities van bovenstaande en andere genoemde termen in dit document zijn te vinden in hoofdstuk 5, bijlage 1.

Om effectief beleid op deze onderwerpen te formuleren, is een gestandaardiseerde manier van het classificeren van data essentieel. Dataclassificatie is het op basis van bepaalde kenmerken categoriseren van data om vervolgens vast te kunnen stellen hoe de data moeten worden behandeld, opgeslagen, beveiligd en gedeeld. Door het toekennen van een bepaalde waarde aan data is duidelijk op welke wijze met deze data moet worden omgegaan.

Deze standaard biedt Umc's een uniforme methode om data te classificeren en op basis daarvan bijpassende vertrouwelijkheidslabels en sub-labels toe te kennen. Deze labels kunnen worden toegepast op zowel gestructureerde als ongestructureerde data en dienen als basis voor het opstellen van passend beleid binnen de verschillende domeinen van data governance.

1.2 Toelichting veelgebruikte termen

Ter bevordering van het begrip van de standaard is het belangrijk om een uniforme definitie aan te houden. Op basis van deze definitie is in hoofdstuk 5, bijlage 1, de definitielijst te vinden. Passend bij dit hoofdstuk lichten we een aantal definities uit die beter inzicht geven in het onderwerp.

Dataclassificatie	Dit is het categoriseren van data op basis van vertrouwelijkheid, gevoeligheid en/of andere risicofactoren. De AVG en de Autoriteit Persoonsgegevens benadrukken dat organisaties passende beschermingsniveaus moeten hanteren op grond van het risico. Door classificatie is duidelijk welke beveiligingsmaatregelen nodig zijn.
Gestructureerde data	Data in een vaste indeling, zoals relationele databases of CSV-tabellen, waardoor het eenvoudig door computers kan worden verwerkt. Dit kan bijvoorbeeld patiëntgegevens in een EPD zijn, of transactiegegevens in financiële systemen. Vanwege de structuur is het beheer en zoeken doorgaans makkelijker dan bij ongestructureerde data.
Ongestructureerde data	Dit is data zonder vooraf vastgelegde structuur, zoals e-mails, tekstbestanden, afbeeldingen of social media content. Vaak is deze informatie lastiger te doorzoeken en te beheren dan gestructureerde data. Bij ongestructureerde data is goede classificatie en labeltoepassing extra belangrijk voor beveiliging en vindbaarheid.

1. 3 Doelstelling

Deze standaard beschrijft de inrichting van dataclassificatie en het toekennen van vertrouwelijkheidslabels binnen de Umc's. De standaard draagt bij en geeft invulling aan het waarborgen van de privacy en veiligheid van diverse soorten gegevens. Daarnaast zorgt de standaard voor naleving van relevante wet- en regelgeving. Transparantie en verantwoording met betrekking tot de omgang en de beveiliging van data binnen de Umc's worden eveneens bevorderd. Tot slot ondersteunt de standaard innovaties die bijdragen aan beter databeheer en -beveiliging.

1.4 Belang van dataclassificatie

De Umc's van Nederland zetten met deze standaard in op een uniforme aanpak van dataclassificatie bij datagebruik, waarbij wordt toegezien op:

- **Vertrouwen van patiënten:** Onze patiënten moeten erop kunnen vertrouwen dat hun gegevens veilig en correct worden beheerd. Een gestandaardiseerde aanpak versterkt dit vertrouwen en kan de algehele tevredenheid en betrokkenheid van patiënten, in alsmaar toenemende digitalisering, verbeteren.

- **Bescherming van onze (patiënt)gegevens en andere vertrouwelijke en/of gevoelige informatie:** Umc's beheren enorme hoeveelheden vertrouwelijke en gevoelige (patiënt)informatie. Een gestandaardiseerde aanpak/standaard zorgt ervoor dat deze gegevens consistent worden beschermd tegen datalekken en cyberaanvallen.
- **Efficiëntie en kostenbesparing:** Door een uniforme aanpak kunnen processen met elkaar vooraf gestroomlijnd worden, wat in beginsel kan leiden tot efficiëntere operaties en kostenbesparingen. Dit is vooral belangrijk in een sector waar budgetten vaak onder druk staan. Op deze manier bundelen we de krachten en kennis en kunnen we zo een standaard voor de gehele sector neerzetten.
- **Verbeterde samenwerking:** Een gestandaardiseerde data governance structuur faciliteert de uitwisseling van gegevens tussen de Umc's. Dit bevordert samenwerking en onderzoek, wat kan leiden tot betere patiëntenzorg en innovaties in de medische wetenschap.
- **Naleving van wet- en regelgeving:** Door een uniforme standaard te hanteren, kunnen de Umc's voldoen aan nationale en internationale regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG), UAVG, Cyberbeveiligingswet (Cbw), ISO27001 en NEN7510. Via deze standaard kunnen we een nog betere invulling geven aan de benodigde technische en organisatorische maatregelen die regelgeving vraagt.

1.5 Overwegingen

Deze standaard is geschreven met vooral ongestructureerde data in gedachten, maar de belangrijkste ideeën en uitgangspunten gelden ook voor gestructureerde data. De standaard is opgesteld met het oog op de toekomst zodat deze ook toepasbaar is op nieuwe data die wordt gecreëerd.

Bij het gebruik van (sub)labels zoals 'intern' of 'intern/extern' is het goed om te beseffen dat dit niet betekent dat de informatie automatisch met iedereen gedeeld *moet* worden. De labels helpen juist om te voorkomen dat informatie onnodig breed verspreid wordt, en zorgen ervoor dat delen van informatie op een zorgvuldige en proportionele manier gebeurt.

De volgende hoofdstukken gaan dieper in op de beleidskaders en uitgangspunten rondom dataclassificatie binnen de Umc's. Hier wordt uiteengezet hoe data op basis van specifieke kenmerken wordt gecategoriseerd en welke richtlijnen en regelgeving hierbij van toepassing zijn. Ook wordt besproken welke waarden aan data worden toegekend om te bepalen hoe deze behandeld, opgeslagen, beveiligd en gedeeld moet worden, met nadruk op wettelijke eisen zoals de AVG, UAVG en andere relevante normeringen.

2. Beleidskaders en uitgangspunten

Het classificeren van data is het op basis van bepaalde kenmerken categoriseren van data om vervolgens vast te kunnen stellen hoe de data moeten worden behandeld, opgeslagen, beveiligd en gedeeld. Door het toekennen van een bepaalde waarde aan data weten gebruikers hoe zij met deze data om moeten gaan.

2.1 Beleidskaders voor dataclassificatie

Bij het classificeren van data zijn diverse wet- en regelgeving en normeringen van toepassing. In de wet- en regelgeving en normeringen worden eisen gesteld aan de behandelwijze van data. De volgende wet- en regelgeving en normeringen zijn van toepassing.

- Algemene Verordening Gegevensbescherming (AVG),
- Uitvoeringswet AVG,
- Wet medisch-wetenschappelijk onderzoek met mensen,
- Archiefwet,
- Selectielijst Universiteiten en Universitair Medische Centra 2020
- Cyberbeveiligingswet (Cbw),
- Cyberbeveiligingsbesluit (Cbb),
- ISO27001,
- NEN7510,
- The AI Act - Regulation (EU) 2024/1689

Bovenstaande opsomming is niet limitatief en er kan er ook aanvullend intern beleid zijn.

2.2 Toelichting veelgebruikte termen dataclassificatie

In elke organisatie die met informatiestromen werkt komen we in aanraking met verschillende soorten gegevens. Sommige daarvan zijn hoogst vertrouwelijk en verdienen extra bescherming, terwijl andere juist minder kritisch zijn en eenvoudig(er) gedeeld kunnen worden. Om hier zorgvuldig en uniform mee om te gaan, is het van belang een gemeenschappelijke taal te hebben over de vraag wat we onder ‘gegevens’, ‘persoonsgegevens’, ‘bijzondere persoonsgegevens’ en ‘gevoelige gegevens’ verstaan.

Data (“gegevens”)	Data wordt de ‘grondstof van informatie’ genoemd en informatie wordt ‘data in een context’ genoemd. Vaak wordt een gelaagde piramide gebruikt om de relatie te beschrijven tussen data (aan de basis), informatie, kennis en wijsheid (helemaal bovenaan). [1] Data kan variëren van technische meetwaarden en onderzoeksresultaten tot tekstbestanden, audio-opnames of foto’s. Ook samenvattingen, statistische rapporten of financiële tabellen vallen onder deze brede noemer ‘gegevens’. Eigenlijk gaat het hier om elk stuk informatie dat wordt vastgelegd, bewerkt, uitgewisseld of opgeslagen – ongeacht of het herleidbaar is tot een persoon. In de zorgsector komen we bijvoorbeeld dagelijks in aanraking met medische testresultaten, protocollen, roosters en financiële rapportages. Maar denk ook aan notities in vergaderstukken of rapportages van kwaliteitsmetingen. Al deze gegevens kunnen een andere mate van vertrouwelijkheid hebben en vragen daarom om een passende manier van classificeren en beschermen.

Persoonsgegevens	Zodra de informatie over een natuurlijk persoon (mens) gaat of daaraan te koppelen is, spreken we van persoonsgegevens. Dit is volgens de AVG "*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon*". Het gaat dus om gegevens die direct of indirect naar een individuele persoon te herleiden zijn. We geven hieronder een aantal voorbeelden. • Naam, adres, woonplaats (NAW-gegevens) • Geboortedatum, geslacht, nationaliteit • E-mailadres of telefoonnummer • Patiëntnummer, BSN, omdat deze nummers te herleiden zijn tot een natuurlijk persoon • IP-adres, mits dat nummer direct of indirect te herleiden is tot een natuurlijk persoon • Informatie over iemands zorgverzekering of behandeltraject, voor zover dit relateert aan een persoon
Bijzondere persoonsgegevens	Niet alle persoonsgegevens hebben dezelfde gevoeligheid. Bijzondere persoonsgegevens vormen een aparte categorie. In de AVG worden hieronder verstaan: '*gegevens over iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, genetische gegevens, biometrische gegevens voor identificatiedoeleinden, gezondheidsgegevens en gegevens over iemands seksueel gedrag of seksuele gerichtheid*'. Deze gegevens krijgen extra bescherming, omdat het risico op discriminatie, stigmatisering of inbreuk op de persoonlijke levenssfeer bij deze categorie veel groter is.
Gevoelige gegevens	Naast persoonsgegevens (inclusief de bijzondere) bestaan er gevoelige gegevens die niet per se herleidbaar zijn tot een specifieke persoon, maar die wél vertrouwelijk of strategisch van aard zijn. Denk bijvoorbeeld aan de volgende soorten gegevens. • Financieel gevoelige gegevens: zoals interne budgetprognoses, contracten met zorgverzekeraars of offertes van leveranciers. • Juridisch gevoelige gegevens: bijvoorbeeld (concept)overeenkomsten, processtukken en informatie over lopende rechtszaken. • Concurrentiegevoelige bedrijfsinformatie: strategische plannen, research- en innovatiedocumenten, of gedetailleerde beleids- en jaarplannen die niet openbaar zijn. • Operationele gegevens: bijvoorbeeld veiligheidsprotocollen, incidentrapportages of nog niet-gepubliceerde onderzoeksresultaten. Hoewel de categorie 'gevoelige gegevens' niet in alle gevallen onder de AVG of medische wetgeving valt – omdat ze vaak niet direct over individuele personen gaat – kan de impact op de organisatie groot zijn als dergelijke data ongewenst openbaar wordt. De reputatie van het instituut, de strategische positie of financiële belangen kunnen hierdoor worden geschaad.

2.3 Verantwoordelijkheden bij dataclassificatie

Het beleggen van verantwoordelijkheden bij dataclassificatie is randvoorwaardelijk omdat het zorgt voor duidelijkheid over wie verantwoordelijk is voor het uitvoering geven aan bescherming van verschillende soorten gegevens. Door verantwoordelijkheden duidelijk te definiëren, wordt transparantie en verantwoording binnen het Umc versterkt. De verantwoordelijkheden voor de realisatie van deze standaard, zijn verder uitgewerkt in een RACI tabel, zie hoofdstuk 5, bijlage 2.

2.4 Uitgangspunten voor dataclassificatie

De volgende uitgangspunten worden voor data classificatie gehanteerd:

- Dataclassificatie wordt toegepast op gestructureerde en ongestructureerde data.
- Data wordt geclassificeerd op basis van vooraf vastgestelde kenmerken of vertrouwelijkheid (bijvoorbeeld financieel, medisch, persoonlijk, gevoeligheid);
- De data-verantwoordelijke is verantwoordelijk voor het classificeren van de data;
- Passende beveiligingsmaatregelen worden op basis van de vastgestelde dataclassificatie geïmplementeerd;
- Door het toepassen van dataclassificatie kan een organisatie voldoen aan het waarborgen van gecontroleerde toegang tot de data;
- Een uniforme werkwijze voor het toepassen van dataclassificatie draagt bij aan een veilige en efficiënte uitwisseling van informatie, zowel binnen het eigen Umc als met de andere Umc’s alsook met externe partners;
- Het toepassen van dataclassificatie draagt bij aan compliant zijn aan relevante wet- en regelgeving en normeringen (zie paragraaf 2a)

Het volgende hoofdstuk richt zich op vertrouwelijkheidslabels en sub-labels die worden toegepast bij dataclassificatie. Deze labels zijn bedoeld om zowel de vertrouwelijkheid als het juiste gebruik van data voor gebruikers inzichtelijk te maken, en ze vormen een belangrijke stap in het waarborgen van een uniforme en veilige werkwijze binnen de Umc’s.

3. Vertrouwelijkheidslabels en sub-labels

Bij het classificeren van data wordt een vertrouwelijkheidslabel aan de data toegekend. Door het toekennen van een vertrouwelijkheidslabels is voor gebruikers duidelijk wat de vertrouwelijkheid van de data is. Door het toekennen van aanvullende sub-labels wordt voor gebruikers duidelijk op welke wijze zij met deze data om moeten gaan. Dit hoofdstuk beschrijft de vertrouwelijkheidslabels, de sub-labels en de basis afspraken om een uniforme werkwijze voor dataclassificatie binnen de Umc's mogelijk te maken.

3.1 Vertrouwelijkheidslabels

Bij het classificeren van data kan op basis van de kenmerken van de data (type, inhoud, gevoeligheid en/of gebruik van de data) een vertrouwelijkheidslabel worden toegekend. Binnen deze standaard zijn vier vertrouwelijkheidslabels vastgesteld.

Label	Definitie	Voorbeeld(en)
Openbaar	Data die toegankelijk is voor iedereen.	Openingstijden van een ziekenhuis op de website van het ziekenhuis, voorlichtingsmateriaal, een plattegrond van het ziekenhuis, de jaarverslagen, openbare onderzoeksresultaten en algemene informatie over activiteiten van het Umc.
Laag Vertrouwelijk	Data die beschikbaar is voor medewerkers binnen het Umc, maar die niet openbaar is.	Personeelshandboeken, interne gedragscodes/richtlijnen, intern telefoonboek en interne emailadressen en informatiefolders voor nieuwe medewerkers.
Vertrouwelijk	Data die persoonlijke of andere gevoelige informatie bevat en beschermd moet worden tegen ongeautoriseerde toegang.	Interne rapporten, persoonlijke informatie, (gepseudonimiseerde) onderzoeksdata en subsidieovereenkomsten.
Zeer vertrouwelijk	Data die medische of zeer gevoelige informatie bevat en beschermd moet worden tegen ongeautoriseerde toegang.	Patiëntgegevens, bijzondere persoons- of financiële gegevens van studieparticipanten en medewerkers/ studenten, bedrijfsstrategieën, financiële gegevens, intellectueel eigendom, patentaanvragen en andere gegevens die, indien openbaar gemaakt, de organisatie en/ of haar stakeholders/ betrokkenen kunnen schaden.

In hoofdstuk 5, bijlage 4, is een overzicht opgenomen van documenttypen en vertrouwelijkheidslabels.

3.2 Sub-labels

Sub-labels kunnen worden gebruikt om aanvullende kenmerken toe te voegen aan het vertrouwelijkheidslabel. Deze aanvullende kenmerken geven een verdere specificatie van de wijze waarop data beheerd en gedeeld kan worden. Sub-labels zijn van belang om een gradatie in toegangs- en gebruikersrechten toe te kunnen voegen, waardoor de data beschermd wordt en alleen geautoriseerde gebruikers toegang hebben.

Binnen deze standaard zijn drie sub-labels gedefinieerd om de maximale reikwijdte aan te geven:

Alleen intern	Data die alleen bedoeld is voor medewerkers binnen het eigen Umc, deze data mag niet met mensen buiten het Umc worden gedeeld.
Intern en Extern	Data die je voor specifieke doeleinden moet delen met mensen buiten het Umc, zoals andere Umc's, zorginstellingen, externe leveranciers, niet-zorgverleners en/of specialisten. Deze data is vertrouwelijk en moet op een beveiligde manier worden uitgewisseld.
Specifieke gebruikers	Data die alleen bedoeld is om te delen met een groep medewerkers die de verantwoordelijke specificeert. De data-verantwoordelijke bepaalt welke rechten deze personen krijgen, rechten om de data te lezen en/of te bewerken.

De maximale reikwijdte bepaalt de grenzen waarbinnen een groep ontvangers valt. Het uitgangspunt is om sub-labels in te zetten bij de labels *Vertrouwelijk* en *Zeer Vertrouwelijk*. Indien gewenst kunnen sub-labels worden ingezet voor alle vertrouwelijkheidslabels. In hoofdstuk 5, bijlage 3, is een overzicht opgenomen met uses cases gerelateerd aan de gedefinieerde sub-labels.

3.3 Basis afspraken voor vertrouwelijkheids- en sub-labels

De Umc's streven naar een uniforme aanpak van dataclassificatie om zo de samenwerking tussen de Umc's te stroomlijnen en te verbeteren. Daarom is het belangrijk om basis afspraken vast te stellen zodat bij toegekende vertrouwelijkheids- en sublabels door ieder Umc dezelfde maatregelen worden getroffen.

Door het toekennen van een vertrouwelijkheidslabel in combinatie met een sub-label kunnen gerichte beveiligingsmaatregelen worden genomen. De toegang tot data maar ook de deelbaarheid van data kan in meer detail worden gespecificeerd. Daarnaast kan de verspreiding van data beperkt worden, waardoor het risico op ongeautoriseerde toegang of datalekken wordt geminimaliseerd.

De te treffen maatregelen zijn afhankelijk van het type data en de wijze van data uitwisseling.

In onderstaande tabel zijn de basis afspraken vastgelegd voor ongestructureerde data.

Vertrouwelijk-heidslabel	Sub-label	Mag data bekijken	Kan data delen	Mag data verwijderen	Kan data opslaan	Kan label toevoegen/ verwijderen
Openbaar		Ja	Ja	Ja	Ja	Ja
Laag vertrouwelijk		Ja	Ja	Ja	Ja	Ja
Vertrouwelijk	Intern en Extern	Ja	Ja	Ja	Ja	Ja *3
	Alleen intern	Ja	Ja	Ja	Ja	Ja
	Specifieke gebruikers	Ja	Nee *1	Ja	Ja	Ja *3
Zeer vertrouwelijk	Intern en Extern	Ja	Nee *1	Ja	Nee *2	Ja *3
	Alleen intern	Ja	Ja	Ja	Ja	Ja *3
	Specifieke gebruikers	Ja	Nee *1	Ja	Ja	Ja *3

**1 Met data delen bedoelen we verspreiden van kopieën aan derden. Dit kan bijvoorbeeld door papier, mail, USB, fileshare, etc. Doorsturen van e-mail niet mogelijk door ontvanger. Bericht is alleen bedoeld voor de ontvanger(s) en niet daarbuiten. Printen niet mogelijk i.v.m. risico dat de gebruiker de print laat liggen en informatie lekt.*
**2 Externe ontvanger mag het bestand/e-mail niet opslaan.*
**3 Label mag aangepast worden, bij opgaaf van reden. Hiermee wordt gelogged waarom de persoon de label heeft verwijderd/aangepast.*

Dataclassificatie speelt een cruciale rol in het beschermen van gevoelige informatie en het naleven van vastgestelde standaarden binnen Umc's. Door middel van verantwoordelijkheid, governance, bewustwording en adoptie kunnen organisaties een solide basis leggen voor een effectieve aanpak. Het volgende hoofdstuk belicht deze onderwerpen en biedt praktische handvatten voor de implementatie van dataclassificatie.

4. Invoering dataclassificatie

Een effectieve adoptiestrategie vereist een holistische benadering die verantwoordelijkheden, bewustwording, training, ondersteuning, monitoring en continue verbetering omvat. Door deze stappen te volgen, kunnen Umc's ervoor zorgen dat hun medewerkers goed zijn uitgerust om gevoelige informatie te beschermen en te voldoen aan de NFU standaard. Dit hoofdstuk beschrijft de stappen die nodig zijn om een effectieve adoptiestrategie te ontwikkelen en uit te voeren voor dataclassificatie.

Stap 1: Verantwoordelijkheid en governance

Deze standaard en de toekomstige implementatie hiervan is niet alleen een ICT aangelegenheid, maar vraagt een effort vanuit het hele Umc. Eigenaarschap en verantwoordelijkheid zijn in beginsel tweeledig. Enerzijds is een stukje techniek nodig om de standaard te realiseren. Anderzijds ligt er een verantwoordelijkheid bij de bestaande data-gebruikers en medewerkers. Zij zijn namelijk altijd al verantwoordelijke geweest voor de data en de omgang met deze data. De implementatie van deze standaard zal ertoe leiden dat men mogelijk extra bewust van de verantwoordelijkheid zal worden. Dit komt doordat men dient te identificeren welke ongestructureerde informatie er binnen het Umc aanwezig is, hoe dit gebruikt dient te worden en wat de omgangs- en toegangsvormen zijn m.b.t. deze informatie. Daarnaast dienen medewerkers de informatie/documentatie te voorzien van het juiste vertrouwelijkheidslabel, zodat er op de juiste manier mee om wordt gegaan. Hierbij is een goede communicatie richting deze gebruikers van groot belang.
De standaard dient aan te sluiten bij bestaande richtlijnen voor databeheer, privacy en informatieveiligheid. Aanbevolen wordt om deze standaard te vertalen naar intern Umc beleid waarbij aansluiting wordt gezocht met bestaande beleidsdocumentatie.

Stap 2: Adoptie en bewustwording

Dit draagt bij aan een vergroot databewustzijn binnen de organisatie ten aanzien van dataclassificatie. Databewustzijn is echter breder en is een onderwerp op zichzelf binnen data governance.

Bewustwording
Het is belangrijk om alle medewerkers tijdig te informeren over de noodzaak en voordelen van dataclassificatie. Dit kan door middel van interne communicatiekanalen zoals nieuwsbrieven, intranet en e-mails.

Adoptie
Het is cruciaal om trainingsprogramma's te ontwikkelen die zijn afgestemd op de verschillende persona binnen de Umc's (Gezamenlijk personamodel NFU). Maak een onderscheid naar de behoeftes van zorgverleners, onderzoekers en overige medewerkers.
Daarnaast kunnen e-learnings worden geïntroduceerd of aangepast, zodat medewerkers deze op elk gewenst moment kunnen volgen. Het is belangrijk dat deze modules interactieve elementen bevatten om de betrokkenheid te vergroten. Verder kunnen regelmatige workshops en seminars worden georganiseerd om diepgaande kennis over vertrouwelijkheidslabels te bieden, waarbij ook externe experts worden uitgenodigd om hun inzichten te delen.

Ondersteuning
Om medewerkers te ondersteunen bij gegevensbeveiliging, richt een helpdesk/servicedesk in die vragen en problemen kan behandelen. Zorg daarnaast voor toegankelijke documentatie en handleidingen met stap-voor-stap instructies voor het gebruik van vertrouwelijkheidslabels en instrumenten voor data loss prevention (DLP), zodat medewerkers gemakkelijk begrijpen hoe ze deze beveiligingsmaatregelen kunnen toepassen.

Stap 3: Monitoring en evaluatie

Om de adoptie te optimaliseren, is het essentieel om te monitoren en feedbackmechanismen te implementeren. Door regelmatig enquêtes en focusgroepen te gebruiken, kan input worden verzameld en kunnen trainingsprogramma's continu worden verbeterd. Regelmatige evaluaties en aanpassingen van de adoptiestrategie, gebaseerd op feedback en veranderende behoeften, zijn cruciaal.

Monitoring
Monitoring is een doorlopend proces waarbij de geclassificeerde data regelmatig wordt gecontroleerd om ervoor te zorgen dat de classificatie up-to-date blijft en voldoet aan de veranderende regelgeving en bedrijfsbehoeften. Proactief monitoren zorgt voor een snelle identificatie van incidenten, fouten en risico's waardoor direct actie kan worden ondernomen.
Monitoring vindt plaats op basis van risicoanalyse. Een risicoanalyse helpt bij het identificeren van data die een hoog risico vormt voor de organisatie als deze niet goed wordt gemonitord en beschermd. Op basis van de vastgestelde labels en sub-labels kan worden vastgesteld welke data hoger risico heeft en vraagt om monitoring. Een overzicht van te monitoren data wordt vastgelegd waarbij wordt beschreven welke acties ondernomen moeten worden (events).

Verantwoordelijkheden (eerste, tweede en derdelijns) met betrekking tot monitoring zijn vastgelegd in onderstaande RACI-tabel.

Taken	Raad van bestuur	Directeur ICT	Data-verantwoordelijke	Technisch beheerder	Informatie-management	Beheerder Monitoring
Beleid Monitoring	A	C	R	C	R	C
Bepalen/ instellen/ aanpassen parameters Monitoring		R	A	R	R	C
Monitoring van Data		R	A	C	R	R
Registratie/ oplossen events Monitoring			A	C	C	R
Evaluatie/ Monitoring		R	A		R	C
Uitvoeren van opvolgende acties		I	C	R	R	A

Welke events dienen te worden gemonitord is afhankelijk van de gestelde KPI's om de organisatiedoelstellingen te behalen. Deze KPI's worden gerapporteerd in (management) rapportages.

Evaluatie

Op basis van de resultaten van de monitoring van events wordt op regelmatige basis bekeken of de monitoring en de genomen maatregelen (nog) in voldoende mate voldoen aan de eisen van de het Umc en voldoende effectief zijn. Dit kan door het instellen van periodieke controles, audits of evaluatie/assessments. Ook wordt gekeken naar mogelijke trends. Er wordt gerapporteerd over de KPI's, monitoring en trends in (management)rapportages. Aan de hand van de resultaten worden waar nodig aanpassingen in de beheersmaatregelen en monitoring doorgevoerd.

De conclusie van dit hoofdstuk is dat effectieve monitoring en evaluatie essentieel zijn om organisatiedoelstellingen binnen het Umc te behalen. Door KPI's, regelmatige audits en trendanalyses te gebruiken, kunnen organisaties hun maatregelen blijven toetsen en aanpassen. Daarnaast is een robuuste governance-structuur en naleving van regelgeving, zoals de AI Act en Cyberbeveiligingswet, cruciaal voor databeveiliging en compliance.

5. Bijlagen

Bijlage 1: Definities

Daar waar mogelijk is er gebruik gemaakt van bestaande definities. Hierbij zijn onder andere de volgende bronnen gebruikt: Autoriteit persoonsgegevens, Ministerie VWS, DAMA DMBOK.

AI Act (Regulation (EU) 2024/1689)
Dit is de Europese verordening die regels stelt voor het ontwikkelen, gebruiken en verhandelen van AI-systemen binnen de EU. Ze beoogt onder meer risicobeheersing, transparantie en verantwoordelijkheid rond kunstmatige intelligentie. De AI Act is nog in ontwikkeling en kan de wijze van dataverwerking en -beveiliging in zorginstellingen beïnvloeden.

Archiefwet
Deze Nederlandse wet regelt hoe overheidsorganisaties (waaronder Umc's) hun archieven moeten beheren, bewaren en zo nodig overdragen. Het doel is dat belangrijke informatie duurzaam bewaard blijft en toegankelijk is voor raadpleging. Er staan eveneens bewaar- en vernietigingstermijnen in omschreven.

Bijzondere persoonsgegevens
Bijzondere persoonsgegevens zijn gegevens met een extra hoog privacyrisico, zoals ras, religie, gezondheid of seksuele gerichtheid. De AVG geeft hieraan speciale bescherming omdat misbruik of ongewenste openbaarmaking grote gevolgen kan hebben. Voorbeelden zijn medische dossiers en biometrische gegevens voor identificatie.

Cyberbeveiligingsbesluit
Dit besluit werkt de Nederlandse Cyberbeveiligingswet verder uit met operationele regels en voorschriften. Het biedt onder meer nadere kaders over de beveiligingsmaatregelen en meldplichten voor organisaties die onder de wet vallen. Zo moet de digitale weerbaarheid worden verhoogd en continuïteit van vitale processen gewaarborgd.

Cyberbeveiligingswet
Deze wet regelt de Nederlandse implementatie van de Europese richtlijn inzake netwerk- en informatiesystemen (NIS-richtlijn). Ze stelt eisen aan digitale dienstverleners en aanbieders van essentiële diensten, waaronder meldplicht bij ernstige cyberincidenten. Doel is het versterken van de cyberweerbaarheid en het beschermen van vitale infrastructuur.

Data
Data worden de 'grondstof van informatie' genoemd en informatie wordt 'data in een context' genoemd. Vaak wordt een gelaagde piramide gebruikt om de relatie te beschrijven tussen data (aan de basis), informatie, kennis en wijsheid (helemaal bovenaan). [2]
Data kan variëren van technische meetwaarden en onderzoeksresultaten tot tekstbestanden, audio-opnames of foto's. Ook samenvattingen, statistische rapporten of financiële tabellen vallen onder deze brede noemer 'gegevens'.

Data governance
Data governance betreft het geheel aan beleidsregels, verantwoordelijkheden en procedures om de kwaliteit, veiligheid en beschikbaarheid van data te waarborgen. Het omvat onder andere datakwaliteit, eigenaarschap, dataclassificatie en naleving van wet- en regelgeving. Door goede data governance kan een organisatie data effectief, veilig en compliant inzetten.

Data Loss Prevention (DLP)
DLP is een set maatregelen en technologieën om ongeautoriseerde toegang, verspreiding of vernietiging van gevoelige data te voorkomen. Het scant en blokkeert bijvoorbeeld het versturen van vertrouwelijke informatie naar onbevoegde ontvangers. Zo helpt DLP om datalekken proactief te signaleren en te beperken.

Data-lifecycle management
Hiermee wordt het beheer van data gedurende de gehele levenscyclus bedoeld: van creatie en opslag tot archivering en vernietiging. Het zorgt ervoor dat data op elk moment de juiste behandeling, bescherming en retentie krijgt. Hierdoor wordt voldaan aan wet- en regelgeving en blijft data actueel en bruikbaar.

Data-eigenaar / data-verantwoordelijke
De data-eigenaar (of data-verantwoordelijke) bepaalt het doel en de middelen van de dataverwerking. Deze rol is eindverantwoordelijk voor de kwaliteit, beveiliging en juiste omgang met data. De begrippen sluiten aan bij het ‘verwerkingsverantwoordelijke’-begrip uit de AVG, maar zijn breder toepasbaar binnen data governance.

Databewustzijn
Dit is het bewustzijn bij medewerkers dat data van waarde is en op de juiste manier beveiligd en beheerd moet worden. Het omvat kennis van de gevoeligheid van data, relevante wetgeving en de consequenties van onzorgvuldig handelen. Verhoogd databewustzijn ondersteunt een veiligere en efficiëntere datacultuur.

Dataclassificatie
Dit is het categoriseren van data op basis van vertrouwelijkheid, gevoeligheid en/of andere risicofactoren. De AVG en de Autoriteit Persoonsgegevens benadrukken dat organisaties passende beschermingsniveaus moeten hanteren op grond van het risico. Door dataclassificatie is duidelijk welke beveiligingsmaatregelen nodig zijn.

DPIA (Data Protection Impact Assessment)
Een DPIA is een systematische toets om privacyrisico’s rond de verwerking van persoonsgegevens te identificeren en te beperken (art. 35 AVG). Organisaties zijn verplicht een DPIA uit te voeren als de verwerking waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van betrokkenen. Het helpt bij het tijdig nemen van passende maatregelen.

Gegevens
Zie Data.

Gestructureerde data
Data in een vaste indeling, zoals relationele databases of CSV-tabellen, waardoor het eenvoudig door computers kan worden verwerkt. Dit kan bijvoorbeeld patiëntgegevens in een EPD zijn, of transactiegegevens in financiële systemen. Vanwege de structuur is het beheer en zoeken doorgaans makkelijker dan bij ongestructureerde data.

Gevoelige gegevens
Gevoelige gegevens zijn vertrouwelijke of strategische gegevens die niet altijd aan een specifieke persoon gekoppeld zijn. Denk aan financiële rapporten, juridische stukken, concurrentiegevoelige informatie of interne protocollen. Ongewenste openbaarmaking kan grote schade berokkenen aan reputatie, concurrentiepositie of financiële belangen van een organisatie.

Incident / datalek
Dit is een inbreuk op de beveiliging die leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens (art. 4 lid 12 AVG). Organisaties hebben een meldplicht richting de Autoriteit Persoonsgegevens als het datalek een risico oplevert voor de betrokkenen. Snelle reactie en afhandeling zijn cruciaal om schade te beperken.

ISO en NEN normen
Dit zijn internationale (ISO) en Nederlandse (NEN) standaarden voor informatiebeveiliging, zoals ISO 27001 en NEN 7510. Ze beschrijven best practices voor het inrichten van managementsystemen rondom informatiebeveiliging. Voor zorginstellingen is met name NEN 7510 relevant, omdat die is toegespitst op de gezondheidszorg.

Metadata (metadata-management)
Metadata is “data over data”: het beschrijft eigenschappen als herkomst, datum, eigenaar of bestandstype. Metadata-management houdt in dat deze beschrijvingen worden beheerd, zodat data vindbaar en interpretabel blijft. Goede metadata is essentieel voor effectief datagebruik, archivering en compliance.

Monitoring (in de zin van monitoring van datagebruik)
Monitoring is het continu of periodiek controleren en vastleggen van hoe data gebruikt, gedeeld en beschermd wordt. Dit kan gebeuren met behulp van toolsets die afwijkingen of risico’s signaleren, bijvoorbeeld rond dataclassificatie of ongeautoriseerde toegang. Het helpt organisaties om beveiliging te verbeteren en te voldoen aan interne en externe eisen.

Ongestructureerde data
Dit is data zonder vooraf vastgelegde structuur, zoals e-mails, tekstbestanden, afbeeldingen of social media content. Vaak is deze informatie lastiger te doorzoeken en te beheren dan gestructureerde data. Bij ongestructureerde data is goede classificatie en labeltoepassing extra belangrijk voor beveiliging en vindbaarheid.

Persoonsgegevens
Persoonsgegevens zijn gegevens die direct of indirect te herleiden zijn tot een geïdentificeerde of identificeerbare persoon. Voorbeelden zijn naam, adres, geboortedatum, telefoonnummer of patiëntnummer. Volgens de AVG mogen deze alleen worden verwerkt als er een geldige grondslag en passende waarborgen zijn.

(Vertrouwelijkheids)label
Dit is een aanduiding, bijvoorbeeld “Openbaar” of “Zeer vertrouwelijk”, die de gevoeligheid van data aangeeft. Op grond van de risico’s en de AVG kan men besluiten data streng te beveiligen of juist vrijer te delen. Labels vormen de kern van dataclassificatie en sturen onder meer toegang, deelbaarheid en bewaartermijnen.

RACI-matrix
RACI staat voor Responsible, Accountable, Consulted en Informed. De matrix geeft voor elke taak aan wie de uitvoerder is (Responsible), wie eindverantwoordelijk is (Accountable), wie geraadpleegd moet worden (Consulted) en wie geïnformeerd wordt (Informed). Een goede RACI-matrix voorkomt onduidelijkheid over rollen en verantwoordelijkheden.

Retentie / bewaartermijn
Dit is de periode waarin data bewaard blijft alvorens het gearchiveerd of verwijderd dient te worden. Zowel de AVG als de Archiefwet stellen dat data niet langer mogen worden bewaard dan noodzakelijk voor het doel. Na afloop van de bewaartermijn moet vernietiging of anonimisering plaatsvinden, tenzij wettelijke uitzonderingen gelden.

Sub-label
Een sub-label is een nadere specificatie binnen een hoofdlabel, zoals “Alleen intern” of “Specifieke gebruikers”. Hierdoor kan onderscheid worden gemaakt in wie toegang heeft en welke verwerkingsvormen zijn toegestaan. Sub-labels zorgen zo voor fijnmazige controle over gevoelige of vertrouwelijke data.

UAVG (Uitvoeringswet AVG)
Dit is de Nederlandse uitwerking van de Algemene Verordening Gegevensbescherming (AVG). De UAVG concretiseert of verduidelijkt bepaalde onderdelen van de AVG voor de Nederlandse context. Zo zijn hierin onder andere bepalingen over de minimumleeftijd voor toestemming en de taken en bevoegdheden van de Autoriteit Persoonsgegevens opgenomen.

Verwerker
Dat is de partij die in opdracht van een verwerkingsverantwoordelijke persoonsgegevens verwerkt (art. 4 lid 8 AVG). De verwerker handelt niet voor eigen doeleinden, maar volgt de instructies van de verantwoordelijke.

Verwerkersovereenkomst
Dit is een schriftelijke overeenkomst tussen de verwerkingsverantwoordelijke en de verwerker, zoals vereist door art. 28 lid 3 AVG. Hierin worden onder meer afspraken gemaakt over beveiliging, meldplichten bij datalekken en bewaartermijnen. Zo wordt gewaarborgd dat de verwerker zorgvuldig en rechtmatig met de persoonsgegevens omgaat.

Verwerkingsverantwoordelijke
Dit is de organisatie of persoon die het doel en de middelen van de verwerking van persoonsgegevens bepaalt (art. 4 lid 7 AVG). Hij draagt de (eind)verantwoordelijkheid voor de naleving van de privacywetgeving.

WGBO (Wet op de geneeskundige behandelingsovereenkomst)
Deze wet regelt de relatie tussen zorgverlener en patiënt, inclusief de rechten en plichten rond medische behandelingen. Ze stelt onder meer vast hoe medische dossiers moeten worden bijgehouden, bewaard en wanneer de patiënt recht heeft op inzage. De WGBO is mede van belang voor het verwerken van gezondheidsgegevens in de zorg.

WMO (Wet medisch-wetenschappelijk onderzoek met mensen)
De WMO stelt eisen aan onderzoek met menselijke proefpersonen, zoals de verplichting tot toetsing door een Medisch Ethische Toetsingscommissie (METC). Deze wet waarborgt dat onderzoek ethisch en rechtmatig plaatsvindt en de rechten van proefpersonen beschermd worden. Privacyaspecten, zoals toestemming en bewaartermijnen, vallen ook onder deze regels.

Bijlage 2: RACI-matrix

De verantwoordelijkheden voor de realisatie van deze standaard, zijn weergegeven in een RACI tabel. Onderstaande RACI tabel geeft, niet limitatief, taken en bevoegdheden weer ten behoeve van de standaard, gelinkt aan de verschillen rollen in een organisatie. De onderstaande invulling is indicatief en afhankelijk van de rollen en posities en de keuzes die een Umc daarin maakt.

De afkorting van we letters horen bij de volgende definitie:

- **R** (Responsible): Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is.
- **A** (Accountable): Degene die eindverantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat. Er is slechts één persoon Accountable.
- **C** (Consulted): Deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd.
- **I** (Informed): Iemand die geïnformeerd wordt over de beslissingen, over de voortgang, bereikte resultaten enz.
-

Taken	Raad van bestuur	Directeur ICT/ CIO	Data-verantwoordelijke	Technisch beheerder	Security / Compliance afdeling	Beheerder DLP Monitoring	Data / Informatie management	Eindgebruiker / medewerker
Zet de NFU data governance security standaard om naar intern Umc beleid.	A	C	C		C		R	
Stelt het interne Umc beleid t.a.v. data governance security vast.	A	R	I	I	C	I	R	I
Zorgt dat het interne beleid en de NFU standaard periodiek wordt geëvalueerd en waar nodig herzien.	A	R	C	C	C	C	R	C
Past de vertrouwelijkheidslabels manueel toe op gegevens (bij creatie/opslaan) .			A	R			C	R
Past de vertrouwelijkheidslabels geautomatiseerd toe op gegevens (na creatie/opslaan).			A	R			C	I
Richt een minimum baseline in t.a.v. dataclassificatie en standaard te treffen maatregelen.			I	A	C	I	R	
Richt maatregelen in voor data loss prevention (DLP) conform de classificatie labels.				R	A	I	C	
Bepaalt de eisen t.a.v. retentie /verwijdertermijnen.			A	R	C	I	C	
Monitort en reageert conform beleid op DLP-events.			A	C	C	R	I	I
Communiceert over beleid data governance security.		A	I	I	R	I	C	I
Zorgt ervoor dat eindgebruiker voldoende kennis hebben om dataclassificatie labels juist toe te passen.	A	R	C	C	C	C	R	I

Bijlage 3: Use cases per Sub-label

In deze bijlage zijn een aantal use cases opgenomen om het gebruik van vertrouwelijkheidslabels en sub-labels verder te verduidelijken. Elke use case gaat uit van een Umc-medewerker (Persona) in een bepaalde functie en/of rol die werkt met data en deze al dan niet moet delen met collega's en of derden.

Sublabel	**Intern en Extern** Het sub-label Intern en Extern wordt toegepast voor gegevens die zowel binnen het Umc als met externe partners gedeeld mogen worden.	
Usecase	***Persona - Pieter (IT-manager)*** Pieter implementeert een monitoringoplossing voor medische apparatuur en deelt technische documentatie over deze apparatuur met de leverancier. De documentatie bevat geen patiëntinformatie maar moet wel gedeeld worden met de leverancier.	***Persona - Dr. Emma (Onderzoeker in Cardiologie)*** Emma werkt samen met een externe universiteit aan een multicenteronderzoek. Zij deelt geanonimiseerde datasets van patiënten met hartfalen om patronen te analyseren. Het delen gebeurt via een platform dat voldoet aan internationale privacy- en datastandaarden.

Sublabel	**Alleen Intern** Het sub-label Alleen Intern wordt toegepast voor gegevens die uitsluitend binnen het Umc mogen worden gedeeld.	
Usecase	**Persona -** ***Linda (HR-manager)*** Linda verwerkt interne rapportages over het verzuim van medewerkers. Deze rapportages zijn alleen toegankelijk voor de HR-afdeling en de directie, omdat ze persoonlijke informatie bevatten over medewerkers en hun gezondheidsstatus.	***Persona - Paul (Afdelingshoofd Chirurgie)*** Paul beoordeelt interne incidentmeldingen van de operatiekamer (OK). Deze meldingen worden gedeeld met het crisisteam en de verantwoordelijke afdelingen binnen het ziekenhuis om verbeteringen door te voeren. De maximale reikwijdte is afdelingen, alleen het crisisteam is een specifieke groep van gebruikers.

Sublabel	**Specifieke gebruikers** Het sub-label Specifieke gebruikers wordt toegepast voor gegevens die alleen toegankelijk zijn voor een specifiek team of een specifieke groep	
Usecase	***Persona - Sofia (Onderzoeker)*** Sofia leidt een studie naar een zeldzame genetische aandoening. Zij en haar team zijn de enige personen die toegang tot de gegevens en resultaten van deze studie mogen hebben, met andere woorden alleen het projectteam kan deze gegevens van de studie inzien en verwerken	***Persona - Kees (Privacy Officer)*** Kees beheert juridische documenten over een lopende rechtszaak. Alleen de juridische afdeling en het bestuur hebben toegang tot deze zeer vertrouwelijke gegevens, zodat de integriteit van de gegevens gewaarborgd blijft.

Toepassen van sub-labels in specifieke ziekenhuisscenario's
In plaats van alleen op persona's te focussen, kunnen sub-labels worden gekoppeld aan concrete situaties binnen een ziekenhuis:

Scenario:	Intern en Extern:	Alleen Intern:	Specifieke Gebruikers:
Patiëntenzorg	Geanonimiseerde patiëntgegevens gedeeld met een extern laboratorium voor specifieke genetische analyses.	Toegang tot het behandelplan en zorggeschiedenis van een patiënt binnen een multidisciplinair team.	Toegang tot medicatiegegevens beperkt tot apothekers en voorschrijvende artsen.
Onderzoek en Innovatie	Onderzoeksdata gedeeld met een externe partner voor gezamenlijke publicaties.	Interne evaluatie van onderzoeksresultaten voor bespreking binnen de onderzoeksafdeling.	Gegevens van een experiment exclusief toegankelijk voor een onderzoeksleider en diens assistenten.
Beveiligingsincidenten	Incidentrapporten gedeeld met een externe auditor die de beveiliging beoordeelt.	Loggegevens van een beveiligingsincident gedeeld met de interne IT-afdeling.	Toegang tot gevoelige juridische correspondentie beperkt tot de juridische afdeling.
Klinische Beslissingen	Een patiënt wordt overgedragen van een Umc naar een ander ziekenhuis. Het behandelteam deelt een samenvatting van de medische geschiedenis en diagnostische gegevens via een beveiligd platform om continuïteit van zorg te garanderen.	Het multidisciplinair team (MDT) bespreekt interne behandelopties voor een patiënt met complexe symptomen. Alleen teamleden hebben toegang tot de medische gegevens.	Een specialist heeft exclusieve toegang tot genetische testresultaten van een patiënt om een behandelplan voor te bereiden.

Bijlage 4: Documenttypen en vertrouwelijkheidslabels

In deze bijlage is een tabel gepresenteerd die de verschillende informatie typen en categorieën geplaatst onder het vertrouwelijkheidslabels waar deze vanuit de basis van toepassing op is. Belangrijk om in acht te nemen dat de content en de inhoud van documentatie leidend is en hierom af kan wijken van onderstaande tabel. Deze tabel is bedoeld als richtlijn om richting te geven aan welke informatie geclassificeerd dient te worden met welk vertrouwelijkheidslabel.

Label	Openbaar	Laag vertrouwelijk	Vertrouwelijk	Zeer Vertrouwelijk
Categorie	*Onderzoeksresultaten:* Gepubliceerde wetenschappelijke artikelen en onderzoeksdata.	*Interne rapporten:* Niet-persoonlijke interne documenten en rapporten die niet publiekelijk beschikbaar zijn.	*Persoonlijke gezondheidsinformatie (PHI):* Gegevens die betrekking hebben op de gezondheid van individuele patiënten, zoals medische dossiers.	*Gevoelige medische gegevens:* Informatie over zeldzame of ernstige aandoeningen die extra bescherming vereisen.
	Algemene statistieken: Gegevens over het aantal patiënten, behandelingen, en samenwerkingen.	*Operationele gegevens:* Algemene operationele informatie die niet direct gevoelige gegevens bevat.	*Personeelsinformatie:* Gegevens over medewerkers, zoals salarisinformatie en personeelsdossiers.	*Strategische bedrijfsinformatie:* Gegevens over strategische plannen en bedrijfsvoering die cruciaal zijn voor de organisatie.
	Financieringsinformatie: Informatie over subsidies en financiering ontvangen voor onderzoeksprojecten.	*Interne trainingsmateriaal*: Documenten en presentaties die intern worden gebruikt voor opleiding en training van personeel.	*Niet-gepubliceerde onderzoeksdata:* Data die nog niet openbaar is gemaakt en vertrouwelijk moet worden behandeld.	*Beveiligingsinformatie:* Details over beveiligingsmaatregelen en protocollen.
	Voorlichtingsmateriaal: Informatie en brochures die beschikbaar zijn voor het publiek, zoals gezondheidsvoorlichting en preventiemateriaal.	*Evaluatierapporten:* Rapporten over de effectiviteit van voorlichtings- en onderwijsprogramma's die niet publiekelijk beschikbaar zijn.	*Studenteninformatie:* Gegevens over studenten, zoals inschrijvingen en prestaties, die niet openbaar gedeeld mogen worden.	*Gevoelige onderwijsgegevens*: Informatie over specifieke onderwijsstrategieën en methoden die cruciaal zijn voor de organisatie.

Bovenstaande categorieën kunnen onderstaande informatie typen bevatten. Deze lijst is niet compleet maar dient als een indicatie voor informatie en documenttypen die in de categorie vallen.

Bijlage 5: Training & Bewustwording

In deze bijlage zijn voorbeelden opgenomen van mogelijke trainingen ter ondersteuning van het adoptietraject.

1. Basiskennis gegevensbeveiliging	
Introductie tot gegevensbeveiliging	Een algemene training die de basisprincipes van gegevensbeveiliging uitlegt, inclusief waarom het belangrijk is en wat de rol van elke medewerker is.
Begrijpen van vertrouwelijkheidslabels	Een algemene training die de basisprincipes van gegevensbeveiliging uitlegt, inclusief waarom het belangrijk is en wat de rol van elke medewerker is

2. Specifieke Trainingen voor Rollen	
Training voor IT-Personeel	Diepgaande sessies over de technische aspecten van DLP en vertrouwelijkheidslabels, inclusief configuratie, monitoring en probleemoplossing.
Training voor Automatiserings(contact)personen van de afdelingen:	Afdelingsspecifieke sessies over (de implementatie van) DLP en vertrouwelijkheidslabels, inclusief configuratie en monitoring.
Training voor beveiligingspersoneel:	Focus op het identificeren en reageren op beveiligingsincidenten, evenals het implementeren van beveiligingsbeleid en -procedures.

3. E-learning Module	
Interactie en quizzen	Modules die interactieve elementen en quizzen bevatten om de kennis van medewerkers te testen en te versterken.
Scenario-gebaseerde Training	Virtuele scenario's waarin medewerkers moeten reageren op verschillende beveiligingsincidenten, zoals een phishing-aanval of een datalek.

4. Workshops en Seminars	
Hands-on workshops	Praktische sessies waarin medewerkers leren hoe ze vertrouwelijkheidslabels en DLP-tools in hun dagelijkse werk kunnen toepassen.
Gastsprekers en experts	Seminars met gastsprekers uit de industrie die hun ervaringen en best practices delen op het gebied van gegevensbeveiliging

5. Regelmatige Opfristrainingen	
Jaarlijkse opfriscursussen	Jaarlijkse trainingen om medewerkers op de hoogte te houden van de nieuwste ontwikkelingen en veranderingen in het gegevensbeveiligingsbeleid.
Ad-hoc trainingen	Trainingen die worden georganiseerd naar aanleiding van specifieke incidenten of veranderingen in de regelgeving.

6. Gamification	
Beveiligingsuitdagingen	Competitieve uitdagingen en spellen die medewerkers aanmoedigen om hun kennis van gegevensbeveiliging te testen en te verbeteren.
Beloningssystemen	Beloningen en erkenningen voor medewerkers die uitblinken in hun kennis en toepassing van gegevensbeveiligingsmaatregelen.