Elektronische gegevens: reglement inzake toegang elektronische gegevens in het patiëntendossier (KWS) - versie 3
Autorisator: Ramaekers, Hans - 17-02-2021
Afgeprinte versie te gebruiken tot 17-02-2023. Of wanneer de elektronische versie eerder wijzigt, dient ook deze versie, al dan niet door de auteur, aangepast te worden.

Activiteiten

Reglement inzake toegang tot gegevens in het elektronisch patiëntendossier van Nexuz Health in Noorderhart

Noorderhart maakt binnen Nexuz Health deel uit van het UZ Leuven netwerk. De algemene regels voor toegang tot elektronische gegevens van dit netwerk zijn daardoor ook van toepassing voor medewerkers van Noorderhart.

Gebruikersnaam en paswoord / wachtwoord

Om van start te gaan op het netwerk heb je een gebruikersnaam en een paswoord nodig:

- De **gebruikersnaam** (login of account) is uniek en wijzigt nooit
- Het **paswoord** bepaal je zelf en is strikt persoonlijk (mag nooitworden doorgeven) . Om de 4 maanden dien je je wachtwoord te wijzigen.
- Nieuwe personeelsleden krijgen een login en paswoord op de eerste werkdag.
- Aanvraag van een gebruikersnaam en paswoord voor anderen dan personeelsleden (Noorderhart medewerkers):
    - de aanvraag wordt gericht aan de dienst IT
    - nodige gegevens zijn: naam, voornaam, geboortedatum, geboorteplaats, rijksregisternummer en dienst(en) waartoe de medewerker toegang moet krijgen
    - de aanvraag gebeurt altijd door de verantwoordelijke van de dienst, per mail of brief (nooit mondeling of via telefoon).
- Met je gebruikersnaam en paswoord heb je standaard toegang tot je Windows werkomgeving, e-mail en standaard netwerkmappen.
- Toegang tot andere applicaties (KWS, ...) en specifieke netwerkmappen dient apart te worden aangevraagd door de dienstverantwoordelijke (je krijgt deze niet automatisch als je een login aanvraagt). Indien voor toegang tot deze applicaties een aparte gebruikersnaam en paswoord is vereist, zijn deze strikt persoonlijk. Het is niet toegelaten om zich toegang te verschaffen tot deze applicaties door gebruik te maken van de gebruikersnaam en het paswoord van een andere gebruiker.
- Bij het eerste gebruik dient het paswoord gewijzigd te worden.

Regels i.v.m. paswoorden

Paswoorden / wachtwoorden zorgen voor beveiliging en afscherming van gegevens en zijn dus ook van enorm belang. Om het voor een mogelijke “inbreker” niet te eenvoudig te maken om uw paswoord te vinden, zijn deze aan een aantal regels onderworpen:

- Je wachtwoord moet minimaal 8 tekens lang zijn.
- Je wachtwoord moet verschillen van de 5 vorige wachtwoorden.
- Je wachtwoord mag niet gelijk zijn aan jouw gebruikersnaam, of meer dan twee opeenvolgende karakters uit de gebruikersnaam bevatten.
- Je moet karakters gebruiken uit minstens 3 van de 4 volgende reeksen (gebruik alleen karakters uit deze 4 reeksen):
    - Kleine letters abcdefghijklmnopqrstuvwxyz
    - Grote letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
    - Nummers 0123456789
    - Andere Tekens ! " # $ % & ' ( ) * + ´ - . / : ; < = > ? @ [\ ] ^ _ `{ | } ~
- Vier opeenvolgende karakters mogen niet hetzelfde zijn.
- Je wachtwoord wordt gecontroleerd aan de hand van een woordenboek:
    - Bestaande woorden van 4 tot 8 tekens mogen niet in je wachtwoord zitten.
    - We gebruiken Nederlandse, Franse, Engelse en Duitse woordenboeken.

    - Je mag woorden gebruiken waarvan je de klinkers vervangt door cijfers vb. waterval -> w8t3rv8l.
- **Iedereen is verantwoordelijk voor wat er onder zijn of haar login gebeurt. Een paswoord is persoonlijk en mag nooit worden doorgegeven of worden opgeschreven**. **Als je een toestel verlaat, log je ook altijd uit.**
- Men kan 7 foutieve pogingen ondernemen om een paswoord in te geven. Na de zevende poging zal uw gebruiker 30 minuten op inactief worden gezet.
- Je paswoord moet om de 4 maanden gewijzigd worden. Nadat het paswoord vervallen is kan men dit nog gedurende 120 dagen wijzigen. Na deze periode wordt de login op inactief gezet. Enkel 'beheerders' kunnen de login terug activeren. Hierbij wordt automatisch een nieuw paswoord gecreëerd. De gebruiker wordt dan gevraagd dit paswoord opnieuw te wijzigen naar een persoonlijk paswoord.

Specifieke regels voor toegang vanuit andere omgevingen dan UZ Leuven

- Voor de toegang tot het UZ Leuven netwerk en KWS binnen de (partner)ziekenhuizen dient authenticatie minstens op basis van ‘something you know’ te gebeuren (d.i. een voldoende sterk paswoord dat vervalt). Bij Single Sign On oplossingen dient hiermee rekening gehouden te worden (bijv. personeelsbadge ‘something you have’ EN paswoord ‘something you know’)
- Het paswoord moet voldoen aan dezelfde policies (of sterker) dan de paswoord policies van het KWS.
- Voor toegang tot het KWS van buiten het ziekenhuis (remote acces) dient de toegang te gebeuren met een extra vorm van ‘strong authenticatie’. Er wordt niet alleen met KWS-login en paswoord ingelogd, maar ook steeds met een Token of E-id.
- De PC’s waarop het KWS wordt uitgevoerd moeten uitgerust zijn met:
    - een recent antivirus programma
    - laatste security patches van Microsoft

Creëren van logins

- Er worden enkel logins gemaakt voor fysieke personen die deze login strikt persoonlijk gebruiken. Er worden dus geen testlogins gemaakt die door meerdere personen gebruikt zouden kunnen worden.
- In specifieke omstandigheden kan een persoon een tweede login krijgen voor testdoeleinden (bv de leden van de implementatieploeg of developpers). Voor deze login gelden dezelfde strikte regels: enkel door die persoon te gebruiken en paswoord nooit doorgeven.

Distributie van paswoorden

- Paswoorden worden enkel individueel aan personen bezorgd. In het systeem is een tool voorzien om login en paswoord op een individueel blad te printen, zodat dit aan de gebruiker kan gegeven worden.
- Nooit worden lijsten met paswoorden doorgegeven, aan prikborden gehangen, via mail doorgestuurd of op enige andere manier ‘gepubliceerd’ waardoor iemand paswoorden van andere gebruikers kan zien.

Gebruik van e-mail, intranet en internet

Het is essentieel dat elke gebruiker op het Inter- en intranet zijn/haar eigen verantwoordelijkheid ten aanzien van websites, systemen en personen draagt. De gebruiker is uiteindelijk zelf verantwoordelijk voor zijn/haar acties op het Inter- en intranet en bij gebruik van e-mail. (zie ook de tekst i.v.m. gebruik van email, intra- en internet, alsook de tekst i.v.m. discretieplicht).

Toegangscontrole in het KWS van Nexuz Health

Uitgangspunten

Noorderhart heeft gekozen voor één centraal dossier per patiënt over alle specialismen heen. Er werd bewust ook geen opsplitsing gemaakt tussen het verpleegkundig, het paramedisch en het medisch dossier. Indien men een patiënt behandelt, krijgt men toegang tot het hele dossier voor de periode dat de behandeling duurt, uitgebreid met een ‘grace period’ waarop verder in dit document wordt ingezoomd. Dit moet de vlotte doorstroming van informatie ondersteunen en een multidisciplinaire aanpak bevorderen.

De KWS-software is dezelfde op alle plaatsen in Noorderhart: op elk werkstation zijn in principe alle functies beschikbaar.

Het is de toegangscontrole die bepaalt wie wat mag zien en wie welke acties mag uitvoeren.

Inloggen in KWS

Om toegang te krijgen tot KWS moet een persoon zich steeds aanmelden onder eigen login en paswoord. Het ter beschikking stellen van de eigen gebruikersnaam en paswoord aan een andere persoon is niet toegelaten.

Alle acties en toegangen in KWS zijn gebaseerd op deze combinatie van login+paswoord. Regelgeving omtrent paswoorden is hierboven beschreven.

Op verschillende plaatsen in KWS wordt de login geregistreerd en kan men (laten) opvragen wie welke gegevens bekeken en/of gewijzigd heeft (steeds bij acties zoals het verzenden, corrigeren en vernietigen van gegevens en in verschillende gevallen bij het opvragen van gegevens).

Iedereen is persoonlijk verantwoordelijk voor de acties die onder zijn login in KWS worden uitgevoerd.

Een scherm kan om die reden ook eenvoudig beveiligd worden. Enkel de hieronder beschreven werkwijzen zijn toegelaten:

- Schermbeveiliging: via de menu optie ‘Algemeen’ – ‘Beveilig scherm’ uit het mededelingenvenster of de shortcut ‘ctrl+B’. Als je daarna als eerste terug inlogt krijg je alle vensters terug zoals ze achtergelaten zijn. Dit past men toe indien men kortstondig de toepassing op dat scherm verlaat. Logt een andere gebruiker in dan worden alle vensters in KWS gesloten. Indien een toestel 15 minuten niet gebruikt wordt dan gaat KWS automatisch in beveiliging.
- Volledig uitloggen: via de menu optie 'Algemeen - Nieuwe gebruiker' of de shortcut 'ctrl+L'
- Sessie doorgeven naar een ander werkstation: via de menu optie ‘Sessie doorgeven’ kunnen gebruikers van een zelfde discipline omloggen met behoud van openstaande vensters.
- Uitbadgen

Toegangscontrole

De toegangscontrole in het KWS bestaat uit 2 luiken: de statische toegangscontrole en de dynamische toegangscontrole.

Statische toegangscontrole

De statische toegangscontrole controleert het verband tussen de (functie van) de gebruiker en bepaalde types gegevens of bewerkingen in het KWS:

"Alleen artsen mogen medicatievoorschriften maken"
"u mag verslagen valideren van het type X"

Meestal worden bewerkingen in het KWS gekoppeld aan functies ("arts", "verpleegkundige", "secretariaat", ...), maar ad hoc regels waar een bepaalde gebruiker een toegang krijgt tot een

bepaalde actie zijn ook mogelijk. Men noemt deze vorm van toegangscontrole "statisch", omdat deze regels zelden wijzigen.

Dynamische toegangscontrole

De dynamische toegangscontrole in het KWS controleert het verband tussen een gebruiker en een patiënt. In principe heeft men geen toegang tot de patiënt, tenzij men bij de behandeling betrokken is. Het KWS kan dit nooit met zekerheid weten maar probeert dit af te leiden. Hiervoor wordt een cascade van regels gebruikt.

Sommige van deze regels zijn erg voor de hand liggend:

> "als de patiënt bij deze gebruiker op consultatie komt"
> "deze gebruiker is als verpleegkundige verbonden aan eenheid X en de patiënt ligt op eenheid X" "er is een contact geregistreerd voor die patiënt waarvoor deze gebruiker assistent of supervisor is".

Andere zijn dan weer complexer:

> "de patiënt moet onderzoek X ondergaan, en u bent supervisor voor onderzoeken van het type Y waaronder onderzoek X valt"

Deze toegangen zijn dynamisch, doordat de toegangen voortdurend veranderen in functie van de gegevens in het dossier. Doordat iemand een aanvraag doet, een afspraak boekt, ... krijgen de personen die hierop actie zullen uitvoeren automatisch toegang. Dit zijn meerdere duizenden wijzigingen per dag.

De cascade van regels die het KWS toepast om automatisch te bepalen of er toegang is tot het volledige dossier van de patiënt is zoals hieronder beschreven:

- De patiënt is nu aanwezig op spoedgevallen en de gebruiker is ook fysiek aanwezig op spoedgevallen.
- De fysieke aanwezigheid van de gebruiker wordt bepaald door het ingelogd zijn op een *geregistreerd toestel* op de locatie spoedgevallen.
- De patiënt is (recent) aanwezig (geweest) op een eenheid en/of afdeling waar de gebruiker standaard toegang tot heeft.
- De patiënt is (recent) aanwezig (geweest) op een eenheid waarvoor de gebruiker een uitzonderlijke toegang voor 1 dag/1 week heeft voor geactiveerd (i.f.v. wachten, dynamisch inzetten vpl op andere eenheden, ...).
- De gebruiker heeft nog een openstaand contact aan hem toegewezen voor deze patiënt
- De gebruiker was toegewezen aan of was de validator (of *geen verslag nodig*) van een contact dat nog geen 14 maanden is afgesloten (zie grace period).
- De gebruiker hoort tot een functiemeting waarvoor deze patiënt een geplande aanvraag heeft openstaan.
- De gebruiker heeft toegang via zeer specifieke regels voor my nexuz pro gebruikers, externe gebruikers, … .

Daarnaast kan een gebruiker ook nog toegang hebben tot een specifiek resultaat (zonder toegang tot het volledige dossier) op basis van zijn postbus en/of de afdruklijst.

Grace period

De dynamische toegang dooft uit na een periode die afhangt van de reden waarom men toegang kreeg. Het is niet zo dat men onbeperkt toegang krijgt tot het *gehele* dossier van een patiënt. Men heeft wel onbeperkt toegang tot het deel van de eigen afdeling, maar toegang tot andere delen van het dossier valt ‘na een tijd’ weg. Zodra de patiënt weer een behandelrelatie heeft met de gebruiker krijgt deze weer toegang tot het hele dossier.

Overrules

Er is een structureel probleem met de implementatie van elke dynamische toegangscontrole: ze is steeds gebaseerd op reeds geregistreerde gegevens (bv. de aanwezigheid van de patiënt). Soms is echter toegang nodig op basis van intentie:

"de patiënt zal bij mij op consultatie komen"
"de patiënt zal door mij geanesthesieerd worden", ...

Ook in geval van nood moet iemand het dossier kunnen openen, zelfs al heeft het KWS geen gegevens waaruit het een behandelrelatie kan afleiden (naast overrule op één dossier bestaat zo ook overrule voor één dag of één week waarmee artsen of verpleegkundigen toegang kunnen krijgen tot alle patiënten van een eenheid of afdeling. Deze mogelijkheid is specifiek voorzien voor wachtdiensten bij artsen of onverwachte vervangingen bij verpleging).

In dergelijk gevallen is een overrule mogelijk: het KWS vraagt een reden en geeft daarna toegang, maar:

- Alleen de dynamische toegangscontrole wordt overruled. Men krijgt toegang tot de patiënt, maar nog steeds met de rechten gekoppeld aan de eigen functie. M.a.w. een verpleegkundige blijft voor het systeem een verpleegkundige, een arts blijft een arts.
- Alle acties die men doet in dat dossier worden in hoge mate van detail gelogd. Het is achteraf perfect controleerbaar wat iemand gezien of gedaan heeft.
- De personen die als supervisor voor een patiënt verantwoordelijk zijn krijgen de lijst met overrules te zien telkens zij een dossier van een van hun patiënten openen. Als ze hierop klikken, krijgen ze de details in de log te zien. Indien zij onregelmatigheden vermoeden, kunnen zij dit via de KWS-implementatieploeg naar de hoofdarts doorgeven.

In bescherming nemen van patiënten en verslagen

Om de dossiers van sommige patiënten beter te beschermen, is het mogelijk om een patiënt in bescherming te nemen. De gebruiker die gegevens van een beschermde patiënt raadpleegt, merkt niets speciaal. Er wordt enkel in een log bijgehouden dat hij/zij toegang heeft gevraagd tot de patiënt én alle acties worden gelogd.

Indien een patiënt in bescherming moet genomen worden, dan verwittigt men de KWS-implementatieploeg.

Medewerkers van Noorderhart zijn standaard ‘beschermde patiënten’.

Log voor bevoegde personen

Supervisoren en bevoegde personen kunnen **gelogde toegangen** (oa overrules) op een patiëntdossier rechtstreeks opvragen **via het dossier** zelf. Bovenaan links op het patiëntdossier staat naast het 'slotje' voor 'volledige toegang' een **knopje** om de lijst met gelogde toegangen op te vragen.

De supervisor kan de gegeven redenen nakijken en indien nodig maatregelen treffen. Elke supervisor beschikt ook over de stored query "ToegewezenOverrules" die voor alle patiënten waaraan hij is toegewezen een overzicht geeft van de bovenstaande doorbrekingen en bijhorende redenen. Deze query is eveneens oproepbaar via het menu “Werklijsten” optie “Overzicht overrules”.

Elke gebruiker (of patiënt) kan via zijn behandelende arts een overzicht krijgen van de bovenstaande doorbrekingen en bijhorende redenen voor zijn eigen patiëntendossier.

Vertrouwelijke en beschermde rapporten

Specifieke laborapporten worden automatisch als confidentieel beschouwd. Het betreft ondermeer HIV en bepaalde cytologische onderzoeken. Deze uitslagen zijn enkel beschikbaar voor de

aanvragers en voor supervisoren en artsen waarvoor een open contact van de betrokken patiënt bestaat.

Verslagen van de dienst Menselijke Erfelijkheid, Psychiatrie en Sociaal Werk kunnen “beschermd” worden. Ze zijn dan enkel beschikbaar binnen deze dienst en voor de contactbestemmelingen van dat verslag. Dit is voor deze diensten beschikbaar omdat hun verslaggeving door de aard van de dienst vaak gegevens van ‘derden’ bevat.

Meta-toegangscontrole

De toegangen van de gebruikers worden onderhouden door gebruikers met meta-toegangscontrole. Deze gebruikers hebben de mogelijkheid hun toegangen tot eenheden en/of afdelingen door te geven of af te nemen van andere gebruikers. Ze beschikken over een overzichtslijst van alle gebruikers die toegang hebben tot hun eenheden en/of afdelingen.

Toegang tot KWS wordt enkel gegeven aan wie het KWS nodig heeft voor zijn/haar functie binnen het ziekenhuis. In principe staat een persoon die toegang heeft tot KWS onder contract: personeelscontract van Noorderhart of partnerziekenhuis, contract als arts met het ziekenhuis, of een individueel contract met het ziekenhuis voor onderzoekers, tijdelijke medewerkers, medewerkers in dienst van artsen.

Anderen zijn (co-)assistenten en stagiairs , stage verpleging, ... waarbij uitgegaan wordt van een verbintenis met de onderwijsinstelling.

In alle andere gevallen dient de toegang tot KWS overlegd te worden met de KWS-implementatieploeg die o.a. op basis van de vraag toegang tot KWS kan afwegen.

Het zetten van toegangen is gebonden aan regels. Hierbij dient steeds de wettelijkheid gerespecteerd. Bv. een secretaresse mag geen toegang krijgen als supervisor (die een arts is) waardoor zij (of hij) verslagen zou kunnen valideren of medicatie voorschrijven. Het diploma van de betrokkene kan hier dus belang hebben. Toegangen dienen ook altijd zo beperkt mogelijk te zijn: wat men nodig heeft in functie van de patiëntengroep en de eigen taakinhoud, maar wel *enkel wat men nodig heeft*.

In elk geval zal ieder die KWS-toegangen beheert dit doen volgens de regels en procedures die binnen UZ Leuven gelden. Als aanpassingen aan deze regels nodig zijn,gebeurt dat in gezamenlijk overleg met de partnerziekenhuizen, zodat voor het ganse systeem steeds dezelfde regels gelden. UZ Leuven blijft hierbij wel de hoofdbeheerder.

Toegang tot beheersmodules van KWS

In de samenwerking met de partnerziekenhuizen is het een basisprincipe dat de partners hun eigen configuraties onderhouden en hun eigen basisgegevens beheren.

Dit gaat o.a. over

- BAS waarin alle afdelingscodes, eenheden en artsen staan
- Toegangsbeheer: maken en beheren van logins
- Toegangscontrole in KWS
- Opnamebeheer
- Beheer zorgmodule
- Beheer van de OKA planner (beheer van OKA zalen, OKA tijd, etc.)
- Beheer van afsprakenboeken
- Beheer van de MZG-toepassing voor het eigen ziekenhuis
- Magister
- KWS-beheer (voor de KWS-implementatieploegen)
- ...

In al deze situaties zullen specifieke medewerkers van de partnerziekenhuizen toegang krijgen tot configuratietools in KWS, BAS of een andere toepassing. Hierdoor hebben zij echter ook toegang tot deze gegevens van UZ Leuven en de andere partners (m.a.w. medewerkers van de partnerziekenhuizen zullen bv. de UZ Leuven bestanden kunnen aanpassen. Afspraak is uiteraard dat niet te doen, maar er zijn geen harde 'muren' die de gegevens van de ziekenhuizen hier scheiden).

Vandaar volgende afspraken voor iedereen die toegang nodig heeft tot een configuratietool:

- Zij volgen voor die specifieke tool een opleiding en stage bij de UZ Leuven verantwoordelijke zoals een UZ Leuven medewerker die zou krijgen
- De UZ Leuven verantwoordelijke voor die tool evalueert de kunde en kennis van die medewerker en beslist over zijn bekwaamheid om op een bepaald moment zelfstandig aanpassingen te mogen doen. In extremis betekent dit dat UZ Leuven kan beslissen iemand geen toegang te geven (zelfde als na een proefperiode van een UZ Leuven medewerker).
- Medewerkers van de partnerziekenhuizen die met een bepaalde tool werken, vormen een team over de ziekenhuizen heen:
    - zij werken volgens dezelfde regels en procedures, UZ Leuven is hoofdbeheerder.
    - aanpassingen worden samen overlegd.
    - zij staan elkaar bij in raad en daad.
    - zij hebben regelmatig overleg.