



9 Regler och styrning av åtkomst till data

Denna checklista sammanfattar vad som bör ingå i dokumentationen av styrning av åtkomst till data.

1 Regler för åtkomst till data

- a) Åtkomst till data får endast ges till säkert identifierade personer
- b) Åtkomst får endast ske till de data användaren har behörighet att ta del av
- c) Stark autentisering ska användas för åtkomst till data
- d) Användare ska vara informerade om säkerhetsrutiner och sekretessregler
- e) Användare ska vara informerade om att efterlevnad av säkerhetsbestämmelser övervakas
- f) Det ska finnas rutiner för tilldelning, förändring och borttagning samt regelbunden uppföljning av behörigheter till data.

2 Tilldelning, förändring och borttagning av behörigheter

2.1 Tilldelning av behörighet

Registerhållare bör beskriva registrets rutiner för tilldelning av behörigheter och information om säkerhet gällande åtkomst av data.

Rutinerna bör beskriva

- a) Hur ansökan om tilldelning ska ske
- b) Vilka uppgifter om användaren som ska registreras för korrekt tilldelning av behörighet
- c) Krav för säker identifiering av användaren
- d) Vem som beslutar om och godkänner tilldelning av behörighet
- e) Hur godkännandet ska ske t.ex. genom signerad ansökan
- f) Hur ansökningshandlingarna sparas (var, papper och/eller elektroniskt)
- g) Hur användaren informeras om säkerhetsrutiner och övervakning av efterlevnad av bestämmelserna
- h) Vart användaren vänder sig om problem uppstår
 - vid inloggning till systemet
 - vid registrering av data
- i) Hur registret får information om användares förändring av arbetsuppgifter som påverkar behörighet till data t.ex.
 - byte av arbetsplats
 - avslutad anställning
 - utökat ansvarsområde för registerarbete
- j) Vilken övrig information som ska distribueras i samband med tilldelning av behörighet, tex. datainmatningsinstruktioner



9 Regler och styrning av åtkomst till data

2.2 Förändring/borttagande av behörighet

Rutinerna för förändring/borttagande av behörigheter bör beskrivas både för situation då användaren eller registerhållaren begär ändringen/borttagandet

- a) Hur begäran om förändring/borttagande ska ske
- b) Vilka uppgifter om användaren som ska registreras för korrekt förändring av behörighet
- c) Vem som godkänner förändringen/borttagandet av behörighet
- d) Hur godkännandet ska ske
- e) Hur ansökningshandlingarna om förändring/borttagning sparas

3 Uppföljning av behörighet

Rutinerna för uppföljning av behörighet bör beskriva

- a) När förändring eller borttagning av behörighet ska göras t.ex. vid
 - byte av arbetsplats
 - utökat/minskat ansvarsområde för registerarbete
 - avslutad anställning
 - överträdelse av säkerhetsrutiner
- b) Regler för när registerhållaren ska ändra eller ta bort behörigheter
- c) Hur dokumentation över användare ska vara med avseende på användaruppgifter såsom
 - användarnamn
 - datum för tilldelning/ändring/borttagning av behörighet
 - behörighetsändring
- d) Hur dokumentationen förvaras och uppdateras och vem som ansvarar för dokumentationen
- e) Kontroll av behörigheter - frekvens och omfattning
- f) Dokumentation av genomförda kontroller med angivande av
 - datum
 - omfattning
 - åtgärder

4 Information om säkerhetsrutiner/innehåll

Rutiner för information om säkerhetsrutiner bör beskriva

- a) Vem som ansvarar för distribution av informationen
- b) När informationen ska distribueras
- c) Hur informationen ska utformas och vilken information som ska adresseras, t.ex.:
 - hantering av användaridentitet och lösenord
 - handhavande av kort (smart card)
 - låsning av dator/utloggning ur datorn



9 Regler och styrning av åtkomst till data

- låsning av rum som lämnas oövakat om utloggning ej gjorts
- hantering av portabel IT-utrustning (t.ex. bärbar dator, USB-minne)
- hantering av personuppgifter i ifyllda pappersfrågeformulär
- hantering av personuppgifter som sparas lokalt på dator
- kontroll av aktiviteter i registret (att loggning sker, på vilket sätt och att uppföljning sker)

5 Referenser

SFS 2008:355, Patientdatalag

SOSFS 2008:14, Informationshantering och journalföring i hälso- och sjukvården, 2 kap., 5-6 §§, 11§

Följande referensdokument finns tillgängliga på Region Skånes hemsida (www.skane.se/infosakbok)

- Handbok för informationssäkerhet
- Slutrapport – Införande av ny patientdatalag, Bilagor 8 och 9

Bilaga 1: Ansökan om tilldelning av användarbehörighet – 3C

Bilaga 2: Ansökan om ändring av användarbehörighet – 3C

Bilaga 3: Ansökan om avregistrering av användarbehörighet – 3C

Bilaga 4: Anvisningar till behörighetsblanketter för 3C-systemet för registrering av data

Bilaga 5: Anvisningar om säkerhetsrutiner

Bilaga 6:

RC Syd, SOP 6, Standard Operating Procedures för externa användare av 3C-systemet på RC Syds registerplattform
Utdrag: Avsnitt 3

Bilaga 7:

RC Syd, SOP 6, Bilaga: Instruktion för externa användare vid användning av 3C-systemet på RC Syds registerplattform
Utdrag: Avsnitt 3-6

9 Regler och styrning av åtkomst till data

Ansökan om tilldelning av användarbehörighet – 3C

Nedanstående person skall ges behörighet som användare av

register:

Personliga uppgifter (var god texta)

Efternamn: Förnamn:

Titel: Avd:

Klinik: Sjukhus:

Tjänsteadress: Postnummer:

Ort:

Tjänste-tel.: Mobil (tillgänglig): Fax:

E-post (tjänste):

Behörighet(er):

Sjukhus/organisation: ☐ läsrätt
☐ läs+skrivrätt

Sjukhus/organisation: ☐ läsrätt
☐ läs+skrivrätt

Sjukhus/organisation: ☐ läsrätt
☐ läs+skrivrätt

Anmälan om tilldelning bekräftas

.....
 Ort och datum

.....
 Registeransvarig (namn och signatur)

.....
 Namnförtydligande

9 Regler och styrning av åtkomst till data

Ansökan om ändring av användarbehörighet – 3C

Ändring av användarbehörighet berör

register:

Användaruppgifter i 3C:

Användarnamn:

Efternamn:

Förnamn:

E-post:

Behörighetsändring gäller:

Från

Sjukhus/organisation: ☐ läsrätt
..... ☐ läs+skrivrätt

Till

Sjukhus/organisation: ☐ läsrätt
..... ☐ läs+skrivrätt

Behörighetsändring ska gälla från och med datum :
År /Månad/Dag

Anmälan om behörighetsändring bekräftas

.....
Ort och datum

.....
Registeransvarig (namn och signatur)

.....
Namnförtydligande

9 Regler och styrning av åtkomst till data

Ansökan om avregistrering av användarbehörighet – 3C

Nedanstående person skall avregistreras som användare av

register:

Användaruppgifter i 3C:

Användarnamn:

Efternamn:

Förnamn:

E-post:

Organisation:

Avregistrering ska gälla från och med datum :
År /Månad/Dag

Anmälan om avregistrering bekräftas

.....
Ort och datum

.....
Registeransvarig (namn och signatur)

.....
Namnförtydligande

9 Regler och styrning av åtkomst till data

Anvisningar till behörighetsblanketter för 3C systemet för registrering av data

Det finns tre blanketter som gäller ansökan om användarbehörighet i 3 C systemet.

1 Tilldelning av användarbehörighet - 3C

- Blanketten används när man ansöker om behörighet första gången.
- Den som ansöker om behörighet fyller i Register, Personliga uppgifter, Behörighet.
- Den som ansöker skickar den ifyllda blanketten till Registeransvarig, eller dennes delegat.
(Om det finns en delegat, så ska denna vara registrerad hos RC Syd: *Registeransvarig måste inkomma till RC Syd med skriftligt dokument att sådan delegat utsetts*).
- Registeransvarig bekräftar att behörighet får utdelas genom att signera blanketten. Den signerade blanketten skickas till RC Syd administration (se kontaktuppgifter).
- RC Syd skapar användarkonto i enlighet med uppgifter i blanketten och distribuerar inloggningsuppgifter till den sökande så snart som möjligt.
Processen kan fördröjas något om RC Syd behöver kompletteringar till ofullständigt/oklart ifylld blankett.

2 Ändring av användarbehörighet - 3C

- Blanketten används när man redan har behörighet till registret men behöver ändra denna behörighet.
- Ändringar kan gälla
 - registreringsrättigheter (läs/läs+skrivrättigheter) och/eller
 - byte av organisationstillhörighet
- Den som ansöker om behörighet fyller i Register, Användaruppgifter, Behörighetsändring och Datum för ändring av behörighet.
- Den som ansöker skickar den ifyllda blanketten till Registeransvarig, eller dennes delegat.
(Om det finns en delegat, så ska denna vara registrerad hos RC Syd: *Registeransvarig måste inkomma till RC Syd med skriftligt dokument att sådan delegat utsetts*)
- Registeransvarig bekräftar att behörighet får utdelas genom att signera blanketten. Den signerade blanketten skickas till RC Syd administration (se kontaktuppgifter).
- RC Syd ändrar användarbehörighet i enlighet med uppgifter i blanketten och distribuerar inloggningsuppgifter till den sökande så snart som möjligt. Behörighetsändringen kan gälla tidigast från det datum som anges i blanketten, men effektueras ev. senare beroende på när blanketten inkommit till RC Syd.

3 Avregistrering av användarbehörighet - 3C

- Blanketten används när en användare inte längre skall ha behörighet till registret.
- Den som ansöker kan vara antingen Användare eller Registeransvarig.
- Den som ansöker om avregistrering fyller i Register, Användaruppgifter, och Datum för avregistrering av behörighet. Den som ansöker kan vara antingen en användare eller Registeransvarig.
- Registeransvarig bekräftar avregistreringen genom att signera blanketten. Den signerade blanketten skickas till RC Syd administration (se kontaktuppgifter).
- RC Syd avregistrerar användaren i enlighet med uppgifter i blanketten .

Notera:

Registeransvariga kan för-ifylla delar av blanketterna (registrets namn/ Behörighetsuppgifter), innan blanketterna delas ut till användare.

Kontaktuppgifter

Postadress

RC Syd
Rörelseorganens forskningsavdelning
Klinikgatan 22, Wigerhuset
Skånes Universitetssjukhus Lund
221 85 Lund

Telefon

046-171348 (sekretariat)
046-17 71 67 (fax)

E-post

pl@rcsyd.se
info@rcsyd.se

9 Regler och styrning av åtkomst till data

Anvisningar om säkerhetsrutiner

RC Syds registerplattform 3C innehåller register som omfattas av personuppgiftslagen. RC Syd har därför utvecklat ett omfattande säkerhetssystem för bevarande av sekretess och dataintegritet. För att systemet skall fungera i sin helhet är det viktigt att du som användare av 3C följer nedanstående säkerhetsrutiner.

- Användaridentitet och lösenord är personliga. Låt inte andra använda uppgifterna.
- Förvara lösenordet på ett betryggande sätt, avslöja det inte för någon annan.
- Logga ut eller aktivera skärmläckare med lösenord när du lämnar datorn.
- Om du använder Smart card för inloggning i 3C, så ska du
 - förvara kortet på ett ur säkerhetssynpunkt tillfredställande sätt
 - både stänga Internet Explorer och ta ut kortet ur kortläsaren för att bli utloggad
- Begär omedelbart nytt lösenord om du misstänker att det avslöjats.

Alla aktiviteter i 3C dokumenteras automatiskt i systemet via loggning och övervakas fortlöpande av RC Syds personal. Loggen innehåller uppgifter

- om åtgärder som vidtagits med data
- tidpunkt för åtgärd
- för vilken patient åtgärden vidtagits
- vem som utfört åtgärden

Personuppgifter som finns på ifyllda frågeformulär ska hanteras som journalhandling, dvs. de ska skyddas mot otillbörlig åtkomst.

Personuppgifter får inte sparas lokalt på portabel IT-utrustning (t.ex. bärbar dator, USB-minne) utan att antingen ha autentiserats eller krypterats för förhindrande av otillbörlig åtkomst. Att endast ta bort personnummer är oftast inte en tillräcklig åtgärd för autentisering.

Portabel IT-utrustning ska hanteras på ett sådant sätt att risken för otillbörlig åtkomst minimeras genom att

- inte lämna utrustningen utan tillsyn under transporter
- förvara utrustningen i låst rum (lägenhet, hotellrum) när den lämnas obevakad.

Kontaktuppgifter

Postadress

RC Syd
Rörelseorganens forskningsavdelning
Klinikgatan 22, Wigerhuset
Skånes Universitetssjukhus Lund
221 85 Lund

Telefon

046-171348 (sekretariat)
046-17 71 67 (fax)

E-post

pl@rcsyd.se
info@rcsyd.se

9 Regler och styrning av åtkomst till data

RC Syd, SOP 6, Standard Operating Procedures för externa användare av 3C-systemet på RC Syds registerplattform
Utdrag: Avsnitt 3

3 Procedurer och instruktioner

I samband med att anslutningsavtal mellan RC Syds och registeransvarig tecknas överlämnas *Instruktion för externa användare vid användning av 3C-systemet på RC Syds registerplattform* till registeransvarig.

Registeransvarig bekräftar att denne har tagit del av instruktionen genom att signera och datera instruktionen.

Instruktion för externa användare vid användning av 3C-systemet på RC Syds registerplattform omfattar procedurer och instruktioner för

- Systemkrav för användning av 3C
- Datainmatning och datahantering
- Handlingsplan vid datorproblem
- Säkerhet
- Utbildning
- Dokumentation

9 Regler och styrning av åtkomst till data

RC Syd, SOP 6, Bilaga: Instruktion för externa användare vid användning av 3C-systemet på RC Syds registerplattform

Utdrag: Avsnitt 3-6

3 Procedurer och instruktioner

3.1 Systemkrav för användning av 3C

3C-systemet är validerat för att användas med Internet Explorer, version 5.0 eller senare. Det är RC Syds ansvar att meddela Registeransvarig för vilken version av Internet Explorer som registret fungerar, och det är Registeransvarigs ansvar att informera användare om detta.

3.2 Datainmatning och datahantering

Data matas in i databasen via en webb-baserad applikation. Efter överföringen meddelas användaren om överförd data har sparats i databasen eller inte. I de fall som data inte sparas finns åtgärder som ska vidtas beskrivna i avsnitt 3.2, *Handlingsplan vid datorproblem*.

Under en datainmatningssession visas aktuellt register och användaridentitet för den inloggade användaren på skärmen. Ingen annan användare får mata in data utan att den inloggade användaren först har loggat ut.

All inmatning och kontroll av data ska göras i enlighet med registerspecifika inmatningsrutiner där sådana finns. Datakontroller som har byggts in i applikationen exekveras automatiskt i samband med inmatning av data.

När inmatningssessionen avslutats ska användaren logga ut och stänga webbläsaren.

För att RC Syds personal ska få genomföra en ändring i data måste en begäran skickas till den registeransvarige för godkännande och arkivering. Registrering av testdata får inte ske i aktivt register.

Hårdkodning av data i databasen accepteras inte så länge databasen är öppen för registrering.

Import av data till databasen får endast ske före inmatningsapplikationen aktiveras för registrering.

9 Regler och styrning av åtkomst till data

3.3 Handlingsplan vid datorproblem

Om en dataöverföring inte lyckas, dvs. data inte sparas i databasen, ska användaren i första hand prova att spara data på nytt. Om problemen kvarstår ska användaren kontrollera att internet-uppkopplingen fungerar.

Om användaren inte kan lösa problemen ska användaren

- vid internet-problem kontakta lokal IT-support
- vid Comporto-relaterat problem kontakta Help Desk på RC Syd (tel. 046-17 13 48)
- tills problemen är lösta spara data i en pappersversion av registerformuläret

4 Säkerhet

4.1 Åtkomstkontroll

Säkerhetsåtgärder som är tillämpliga på 3C-systemet är de som gäller åtkomst av data.

Användarkonton upprättas av RC Syd. Registeransvarig måste kontakta RC Syd för tilldelning, ändring eller återdragande av användarkonto. Begäran om att skrivrättigheter till register i 3C ska återtas ska göras

- för samtliga användare när registerföring av data avslutas
- för enskild användare och specifikt register när användaren inte längre arbetar med registret

Registeransvarig ska ha en lista över vilka personer som har tillstånd att använda 3C-systemet. Listan ska även innehålla information om användarnas organisationstillhörighet, roll och datum för när användarkontot aktiverats/avaktiverats.

Ett nytt användarkonto aktiveras när användaren har erhållit utbildning för 3C-användning för registret, se avsnitt 5 *Utbildning*.

Alla ändringar i databasen sparas i en ändrings-logg. RC Syds personal övervakar åtkomsten av data genom kontroller i ändrings-loggen av

- användaridentitet
- tidpunkt för åtkomst
- till vilken patients uppgifter åtkomsten gäller

Användare ska följa nedanstående säkerhetsrutiner

- användaridentitet och lösenord är personliga och får inte användas av någon annan
- lösenordet ska förvaras på betryggande sätt så att det inte är åtkomligt för annan person

9 Regler och styrning av åtkomst till data

- lösenordet får inte lämnas ut till annan person
- logga ut, eller aktivera skärmläckare med lösenord, när arbetsstationen lämnas obemannad
- vid misstanke om att lösenordet har blivit känt för annan person ska RC Syd meddelas snarast för spärning av lösenordet och distribution av nytt lösenord

4.2 Personuppgiftslagen/Sekretess

Användare ska informeras om att register i 3C-systemet omfattas av Personuppgiftslagen och att uppgifterna skyddas mot obehörig användning, påverkan, och utplåning. Personal som arbetar med registret ska påminnas om gällande sekretessregler.

5 Utbildning

Varje person som ska registrera data i ett register ska ha erhållit relevant utbildning och träning i 3C-systemet för sina uppgifter.

Utbildningsmaterialet omfattar

- 3C Användarmanual
- instruktion för externa användare vid användning av 3C-systemet på RC Syds registerplattform
- eventuella registerspecifika datahanteringsinstruktioner

För träning i 3C-applikationen används ett demonstrationsregister på RC Syds registerplattform. Demonstrationsregistret kan nås genom att vid inloggning uppges

- användarnamn: Demo
- lösenord: omed

6 Dokumentation

Registeransvarig ska se till att en kopia av den godkända och signerade instruktionen skickas till RC Syd för arkivering i projektpärm.