

INTRODUKTION TILL INFORMATIONSSÄKERHET

**För extern personal: konsulter, hyrpersonal,
studenter och hantverkare med flera.**

Inledning

Detta dokument är avsedd för extern personal att ta del av. Extern personal är de som inte har sin anställning i Region Halland, vanligtvis konsulter, hyrpersonal, studenter och hantverkare med mera. I samband med introduktionen på arbetsplatsen ska uppdragsgivaren, chef eller annan utsedd person försäkra sig om att externa medarbetaren tagit del och förstått innehållet i Introduktion till informationssäkerhet. Dokumentet ska också kvitteras genom en underskrift. Kvittensen omhändertas av uppdragsgivaren, projektledaren eller motsvarande.

Informationssäkerhet

Alla som arbetar eller har ett uppdrag i Region Halland ska ha läst, förstått och accepterat innehållet i Introduktion till informationssäkerhet.

En förutsättning för att hälso-, sjuk- och tandvårdens samt övriga verksamheters krav på sekretess och allmän säkerhet ska vara tillgodosedda är att alla användare följer detta regelverk.

Informationssäkerhetspolicy

Region Halland har en [säkerhetspolicy](#) som inkluderar informationssäkerhet.

Behörigheter

Förvaltningschef/verksamhetschef (mot-svarande) är informationsägare och ansvarar för beslut om och tilldelning av behörigheter. Detta gäller vid nyanställning, för nya studerande, vid förändrade uppdrag eller arbetsuppgifter eller vid frånvaro

Gruppenloggning innebär att flera personer gemensamt använder en inloggningsidentitet. Gruppenloggning får undantagsvis tillämpas på de ställen där ett fåtal datorer används av flera personer. Var och en som loggar in ansvarar

för sina egna aktiviteter. Gruppenloggning medger begränsad tillgång till funktioner i regionens nät.

IT- och produktionsmiljö

Underleverantörer, som inte har driftansvar, ska före inloggning i regionens produktionsmiljö informera objektledare IT om syfte, tidpunkt och planerad förändring.

Din dator

Allmänt

Det är förbjudet att ansluta datorer till regionens nät som inte ställts i ordning av IT-service.

Misstanke om virus i program eller datafiler ska omedelbart rapporteras till IT-service.

Behov av att installera program eller tillägg till program lämnas till närmaste chef som hanterar det enligt systemförvaltningsmodellen.

Lämna datorn tillfälligt

När datorn lämnas utan uppsikt ska den låsas.

Efter avslutat arbetspass

Logga ut från nätverket efter avslutat arbetspass. Stäng av datorn efter avslutad arbetsdag om inte någon annan ska använda den och stäng också av skärmen.

Städa skrivbord på datorn

Spara inte dokument direkt på datorns skrivbord. All lagring av dokument ska göras i avsedda kataloger.

E-post

E-post omfattas av samma bestämmelser om offentlighet, sekretess, arkivering med mera, som till exempel traditionella postbefordrade brev och fax. Varje medarbetares e-postlista, det vill säga uppgifterna: e-postadress, avsändare, mottagare, ämnesrubrik, och datum i inkorgen och utkorgen, är allmänna handlingar.

Din e-postadress (...@regionhalland.se) ska inte användas för privat bruk. Att kontakta patienter och förmedla information via e-post är inte tillåtet. Information som omfattas av sekretess, som till exempel journalhandlingar, får inte skickas med vanlig e-post. Endast säker e-post kan användas.

Personnummer får skickas med e-post men aldrig tillsammans med integritetskänslig information som till exempel hälso- och sjukvårdsuppgifter eller personliga omdömen.

Se rutin [E-post](#).

Videomöten

Särskild försiktighet ska beaktas när funktionen dela skrivbord används, då allt som visas på skärmen blir synligt, exempelvis journaluppgifter.

Se rutin [Videokonferens och chatt](#).

Internet

I rutinen [Internet för personal](#) beskrivs hur vi ska förhålla oss surfande på Internet.

AI

Verktyg för generativ AI ska användas med eftertanke. Detta då många av verktygen använder din information för att bygga modellen, vilket kan leda till ett okontrollerat informationsläckage om de används utan eftertanke.

RH ska därför endast använda Microsoft Copilot för att minimera risken för informationsläckage. Information som kan hanteras i Microsoft 365 kan ofta hanteras i Microsoft Copilot.

Lagring av information och lagringsstruktur

Informationen i våra it-system och lagringsenheter tillhör Region Halland och ska vara arbetsrelaterad. G- och H-katalogerna upplevs ibland som privata men det är inte tillåtet att

spara musikfiler, dokument av privat karaktär (till exempel foton) på något av regionens lagringsutrymmen. IT-service har befogenhet att radera dessa filtyper om de sparas på H. Att för privat bruk använda regionens lagringsutrymmen kan leda till arbetsrättsliga åtgärder.

Det är inte tillåtet att lagra information i molntjänster där Region Halland inte har något avtal (exempelvis Dropbox, iCloud, Google Drive).

Patientuppgifter

Patientuppgifter inklusive foton får inte sparas på någon av nedanstående kataloger utan endast i särskilda vårdssystem eller i undantagsfall (digitala bilder) på cd.

C-katalog

Datorns hårddisk ska inte användas för lagring av dokument. Säkerhetskopieras inte.

G-katalog

Här sparas verksamhetsgemensamma dokument och filer.

OneDrive

Lagringsyta i molnet. Används för att lagra och dela information. Ej tillåtet att hantera känslig eller sekretessbelagd information i.

Samarbetsplatser / Teams

På samarbetsplatser kan information som behöver delas av flera lagras. Samarbetsplatser är avsedda för deltagare i projekt, ledningsgrupper, nätverksgrupper etcetera.

Loggkontroll och dataintrång

Arbetsgivarens kontroll

Arbetsgivaren har rätt att få inblick i och kontrollera all information som är lagrad i regionens it-system (även e-post). Ledningen kan därför när som helst kontrollera vad som finns lagrat i regionens lagringsutrymmen.

Loggkontroll

Verksamhetschef eller motsvarande, som har rätt att besluta om behörigheter, ansvarar för att regelbunden kontroll av loggar genomförs enligt rutin.

Dataintrång

Att läsa journal på patient som man inte har vårdrelation med eller inte har behövt uppgifterna för speciella uppdrag betraktas som dataintrång/sekretessbrott. Om loggkontroll visar att du olovligen tagit del av uppgifter kan det leda till polisanmälan eller arbetsrättslig åtgärd.

Se rutin [Misstanke om dataintrång, brott mot tystnadsplikt, it-sabotage](#).

Offentlighetsprincipen

Tryckfrihetsförordningen är en av Sveriges grundlagar. Den ger medborgarna en unik insyn i all offentlig verksamhet, det brukar kallas offentlighetsprincipen. Det här ställer särskilda krav på oss som är anställda i den offentliga sektorn. Vi måste se till att lagen följs, så att alla får möjlighet att utöva sina demokratiska rättigheter.

Tryckfrihetsförordningen är en av våra viktigaste lagar och reglerar hur hanteringen av information ska ske hos en myndighet allt ifrån diarieföring till arkivering av handlingar. Myndighet är i detta sammanhang politisk styrelse/driftnämnd i Region Halland och förvaltningsområde är myndighetsområde.

Förvaltningslagen innehåller krav på service och handläggning.

Sekretess och tystnadsplikt

Offentlighets- och sekretesslagen (SFS 2009:400) innehåller bestämmelser om sekretess i offentlig verksamhet. Huvudregeln är att alla allmänna handlingar är offentliga.

Exempel på undantag är patientjournaler som är allmänna men sekretessbelagda handlingar.

För att skydda patienternas personliga integritet gäller sekretess inom hälso- och sjukvården för uppgift om enskilds hälsotillstånd eller andra personliga förhållanden. Sekretess innebär att det är förbjudet att röja en uppgift, oavsett om man gör det muntligt, skriftligt, genom att lämna ut eller visa handlingar eller på annat sätt. Sekretess gäller inte om uppgiften kan lämnas ut utan att den enskilde eller någon närstående känner obehag av detta, det vill säga en sekretessprövning måste först ha genomförts.

Sekretess kan även gälla andra handlingar som till exempel upphandlingsunderlag, personaladministrativa handlingar med uppgifter om enskilds personliga förhållanden, information inför facklig förhandling samt resultat av genomförda riskanalyser.

Sekretess i folkbokföringen

Uppgifter om personer i folkbokföringen till exempel namn, adress och personnummer, är vanligtvis offentliga. I vissa fall är det viktigt att hindra att en normalt harmlös uppgift lämnas ut. Ett sådant fall kan vara när en person är utsatt för ett hot och därför har behövt skydda sina personuppgifter i folkbokföringsregistret.

Region Halland skyddar normalt endast personuppgifter i sina register om det finns skyddade personuppgifter i folkbokföringsregister, undantag finns (21 kap 3 § OSL)
Se rutin [Sekretess i folkbokföringen](#)

Personuppgifter och dataskydd

Personuppgifter behöver inte vara personnummer utan det räcker med att man kan härleda uppgifterna till en enskild individ.

Enligt Dataskyddsförordningen krävs det en laglig grund för att få registrera

personuppgifter. Region Halland får registrera personuppgifter med stöd av olika lagliga grunder, till exempel när detta är nödvändig för att fullgöra anställningsavtalet mellan dig och arbetsgivaren eller när arbetsgivaren har ett berättigat intresse för behandlingen. Mer information om hur dina personuppgifter behandlas finns att läsa i [Personuppgifter – information till dig som medarbetare](#).

Dataskyddsombud

De personuppgiftsansvariga politiska nämnderna utser dataskyddsombud (DSO), vars uppgift är att se till att dataskyddsförordningens krav uppfylls. DSO-ombuden för bland annat förteckning över personuppgiftsregister och godkänner ansökningar om upprättande av nya register.

Bilaga

Bilaga 1: Kvittens: Introduktion till informationssäkerhet

Bilaga 1 - Kvittens: Introduktion till informationssäkerhet

Sekretess

Sekretess innebär att man inte får berätta eller lämna ut uppgifter om en patient till någon annan än den som deltar i patientens vård – man har tystnadsplikt om vad man vet!

Diskutera därför inte enskilda patients hälsa eller andra personliga förhållanden med någon som inte deltar i patientens vård eller behandling. Detta gäller även om han eller hon i sin tur också har tystnadsplikt.

Sekretessen gäller även efter det att man har slutat arbeta inom hälso- och sjukvården – livet ut.

Det är inte självklart att uppgifter om patienten ska lämnas ut till anhöriga eller närstående.

Fråga vad patienten själv vill eller kontrollera om det finns ett medgivande dokumenterat i journalen. Man ska inte tala om att patienten är inlagd på en vårdavdelning, om det inte tydligt framgår att denna uppgift kan lämnas ut.

Man har inte heller rätt att ta del av dokumenterad information om patienter om man inte deltar i vården av patienten eller på annat sätt behöver uppgifterna för att utföra sitt arbete. Det finns undantag. I vissa fall är man skyldig att lämna ut uppgifter som egentligen är sekretessbelagda. Kontakta närmaste chef eller regionens jurister vid osäkerhet.

Vilka uppgifter gäller sekretessen?

Sekretessen gäller till exempel uppgifter om vem som är patient, den patientens sjukdom och behandling, patientens adressuppgifter, uppgifter om familjeförhållanden och andra sociala förhållanden, arbetsförmåga, arbetsgivare med mera.

Dessa uppgifter finns ofta i patientjournaler eller i anteckningar förda på annat sätt, men sekretessen gäller också sådant som patienterna eller deras närstående själva talat om för personalen.

För vem gäller offentlighets- och sekretesslagen?

Inom hälso- och sjukvården gäller lagen för alla anställda, oavsett befattning och arbetsuppgifter. Sekretessen gäller också studerande och praktikanter.

Brott mot tystnadsplikten

Brott mot tystnadsplikten faller under allmänt åtal och kan ge böter eller fängelse i högst ett år. Mer information om sekretess finns på Intranätet/Rutiner/Sekretess och samtycken.

Kvittens

Jag har läst och förstått vad som avses med sekretess och tystnadsplikt samt tagit del och accepterat innehållet i Introduktion till informationssäkerhet.

Jag förbinder mig att fortsättningsvis följa samt ta del av förändringar och nyheter inom detta område.

Jag förbinder mig att ta del av dokumenterade uppgifter om en patient endast om jag deltar i vården av patienten eller om jag i mitt uppdrag av annat skäl behöver uppgifterna. Jag försäkrar också att jag inte obehörigen ska lämna ut till fysisk eller juridisk person den information som jag får kännedom om i mitt uppdrag inom Region Halland.

.....
Datum

.....
Underskrift

.....
Namnförtydligande och personnummer

Ifylld kvittens sparas hos uppdragsgivaren i 70 år, lämpligtvis i pärm eller i uppdragsgivarens årsakt (diariet)

Uppdaterat från föregående version

Lagt till ett stycke om AI

Föregående versionsuppdateringar

Dokumentet är uppdaterat med nyckelord för att synas på Vårdgivarwebben.