Informationssäkerhet Region Halland

Informationssäkerhet

All verksamhet i Region Halland är i behov av information för att kunna bedrivas ändamålsenligt. Informationen måste därför hanteras säkert. Informationssäkerhet är att säkra att information, i alla dess former, ska finnas tillgänglig när den behövs, att den är korrekt, att obehöriga inte kan få tillgång till den och att händelser i hanteringen av informationen kan spåras. Informationssäkerhet upprätthåller patientintegritet, trygghet för personal och bidrar till god och säker verksamhet. Inom vården är kraven på informationssäkerhet extra höga. Informationssäkerhetsåtgärder ska säkerställa att informationen är försedd med tillräckliga metadata, t.ex. författare, versionsnummer, fastställare, datum för fastställande, för att inga oklarheter kring äkthet eller korrekthet ska behöva uppstå.

Begreppsdefinitioner

Allmän handling
För definition av allmän handling se *Offentlighetsprincipen*. Allmänna handlingar skyddas genom att de registreras i regionens dokument- och ärendehanteringssystem, eller att de hålls ordnade på annat sätt. Det ska klart framgå om de inkommit eller upprättats.

Arbetsmaterial
Såsom framgår i rutinen *Offentlighetsprincipen* är även filer i filserverkataloger eller it-system allmänna handlingar så snart de blivit färdigställda. Då gäller likadana krav på registrering eller annan förvaring som för analoga handlingar. Detta innebär att filerna flyttas från filserverkataloger eller samarbetsytor till system för allmänna handlingar, t.ex. Platina. Filer som behöver bearbetas sparas ner på filserverkatalogen och ska då sparas med minst två positioner i punktnotationen, varav den andra siffran aldrig får vara 0, t.ex. version 5.1. Filer med färdigställda allmänna handlingar punktnoteras alltid med två positioner, varav den andra siffran alltid är noll, t.ex. version 5.0

Information
Information är i detta sammanhang elektroniska handlingar. Kan såväl utgöras av kontorsdokument som fixerade elektroniska informationsmängder i databaser.

Spara/lagra
Förvara filer på ett elektroniskt medium kortare eller längre tid. Hur lång tid avgörs av uppgift i dokumenthanteringsplan eller i enskilt gallringsbeslut. Filerna utgör arbetsmaterial.

Metadata
Betyder data om data och avser uppgifter som behövs för att kunna tolka information i dess rätta sammanhang och för att kunna fastställa dess äkthet. Det kan vara t.ex. författarens namn, tillkomsttidpunkt, vidtagna ändringar, arkivbildare, processtillhörighet osv.

Myndighet
Myndighet är en politisk nämnd/styrelse i Region Halland och förvaltningsområde är myndighetsområde.

Informationssäkerhet i Region Halland

Policies och riktlinjer som styr informationssäkerhetsarbetet

Region Hallands *Säkerhetspolicy* med tillhörande *Riktlinjer för informationssäkerhet och dataskydd* samt *Riktlinjer för säkerhetsskydd* anger inriktning och nivå för informationssäkerhetsarbetet. Utifrån policy, riktlinjer, resultat av riskanalyser, revisioner och informationsklassning tas mål fram som införs i verksamhetsplaner. Även Region Hallands egna samt nationella strategier ska beaktas i arbetet.

Personal

Introduktion till informationssäkerhet för medarbetare

Samtliga personalkategorier som arbetar i och åt Region Halland ska tagit del av introduktion till informationssäkerhet. Närmaste chef ansvarar för att samtliga medarbetare tagit del av *Introduktion till informationssäkerhet*. I Kompetensportalen finns grundläggande utbildningar för informationssäkerhet och dataskydd.

Avslutad anställning

Vid upphörande av anställning ska *Avslutad anställning – checklista informationssäkerhet* användas. Medarbetare ska se till att all verksamhetsinformations har tagits om hand och fördelats innan medarbetaren slutar. Ansvarig chef ska kontrollera detta vid avslutningssamtalet.

Innehåll i användarkonton, exempelvis e-postmeddelanden och filer i personliga kataloger rensas 30 dagar efter avslutad anställning, genom gallringsbeslut.

Lagar och föreskrifter

Offentlighetsprincipen gör att informationen till stor del är allmänna handlingar. Större delen av dessa innehåller mycket känsliga personuppgifter och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen. Detta ställer extra stora krav på hur vi hanterar informationen.
Tillgängligheten till informationen styrs i första hand av:

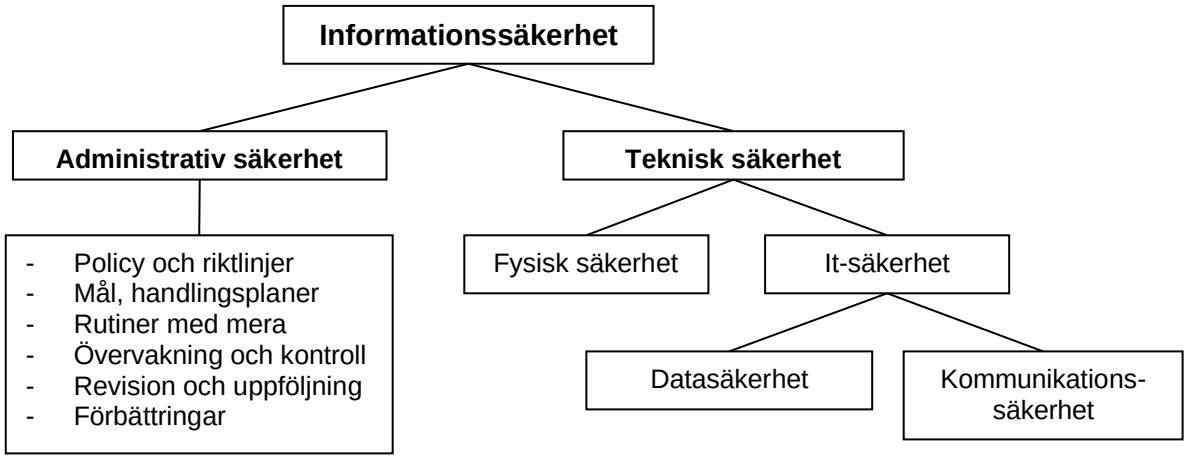
- **Tryckfrihetsförordningen** (1949:105). Här regleras offentlighetsprincipen, det vill säga att offentlig myndighet har skyldighet att lämna ut allmänna handlingar. För privata sektorn föreligger ingen generell skyldighet att lämna ut handlingar.
- **Offentlighets- och sekretesslagen** (2009:400). Här anges vilken information som är sekretessbelagd och alltså undantaget från regeln att myndigheternas allmänna handlingar är offentliga. Sekretess innebär både förbud att röja en uppgift och förbud att lämna ut allmänna handlingar.
- **Arkivlagen** (1990:782). Anger allmänna riktlinjer för bevarande, gallring och arkivering.
- **Hälso- och sjukvårdslagen** (2017:30). Här regleras hur hälso- och sjukvården ska bedrivas så att den uppfyller kraven på god och säker vård. Detta innebär bland annat att vården ska vara av god kvalitet och tillgodose patientens behov av trygghet i vården och behandlingen, vara lättillgänglig, bygga på respekt för patientens självbestämmande och integritet samt främja goda kontakter mellan patienten och hälso- och sjukvårdspersonalen.
- **Patientdatalagen** (2008:355). Här preciseras skyldigheten att föra journal inom hälso- och sjukvården. Lagen ger även möjlighet till sammanhållen journalföring som innebär att vårdgivare via elektroniska system kan ge eller få direktåtkomst till personuppgifter hos en annan vårdgivare.

- **HSLF-FS Journalföring och behandling av personuppgifter i hälso- och sjukvården** (2016:40) kompletterar lagen med mer konkreta anvisningar.
- **Dataskyddsförordningen** (EU 2016/679) syftar till att skydda den personliga integriteten. EU-förordningen preciserar villkor för att behandla personuppgifter inom hälso- och sjukvården.
- **Säkerhetsskyddslagen** (2018:585) innehåller regler om åtgärder till skydd för Sveriges säkerhet
- **Lag om upphovsrätt till litterära och konstnärliga verk** (SFS 2011:94) Immaterialrätt är en sammanfattande benämning på vissa rättsområden som beskriver skydd för till exempel patent och upphovsrätt. Upphovsmannen har ensamrätt till exempelvis bilder, texter och datorprogram och förfogar över rätten att sprida mångfaldiga dessa. Även databaser skyddas genom lagen. Det innebär att det i princip finns förbud för andra att utan tillstånd (licens) från upphovsmannen få kopiera bild, text, datorprogram, databaser eller musik. Respektive förvaltning ansvarar för att förvaltningens programvaror används i enlighet med avtal och licenser. Verksamhetschef/motsvarande tar kontakt med regionjurist vid frågor om upphovsrätt.

Det finns fler lagar och föreskrifter som har betydelse för informationssäkerheten. Se respektive förvaltnings lagförteckning.

Modell för informationshantering

Modellen visar hur information behöver säkras, det vill säga göras tillgänglig och skyddas genom administrativ och teknisk säkerhet. Det mesta i modellen är hämtat från SIS HB 550 Terminologi för informationssäkerhet.



Administrativ säkerhet
Den administrativa säkerheten beskrivs i olika avsnitt/kapitel i ledningssystemet.

Teknisk säkerhet
Den tekniska säkerheten delas in fysisk säkerhet och it-säkerhet.

Fysisk säkerhet
Fysisk säkerhet syftar till att skydda lokaler, utrustning och information.
Fysiskt skydd består av:

- Yttre skalskydd (Mekaniskt skydd i en byggnads omslutningsytor, vars funktion är att förhindra eller fördröja intrång och åverkan.)
- Inre skalskydd (Mekaniskt skydd i en lokals anslutningsytor, vars funktion är att förhindra eller fördröja intrång och åverkan.)
- Kablageskydd
- Bevakning
- Inbrottslarm (Teknisk installation, vars funktion är att upptäcka intrång eller åverkan.)
- Passagekontrollsystem
- Byggnadstekniskt brandskydd (Konstruktions- och installationsskydd som förhindrar och fördröjer brand- och brandgasspridning samt tekniska installationer som upptäcker brand och brandgaser.)

Grundregeln är att information aldrig ska lämnas oskyddad. Utrustning som är känslig i sig själv eller behandlar känslig information, ska placeras och hanteras så att tillträde minimeras. Se respektive förvaltnings kapitel 310 – Säkerhet och krisberedskap.

It-säkerhet
It-säkerhet är teknikens förmåga att förhindra obehörig åtkomst, obehörig eller oavsiktlig förändring, störning vid databehandling samt vid dator- och telekommunikation.
Tekniken ska säkra att vi får tillgång till, kan hantera och kommunicera information, samtidigt förhindra att obehöriga inte kan komma åt den. It-säkerhet består av:

- Datasäkerhet
  Säkerhet för skydd av it-system och dess data som syftar till att förhindra obehörig åtkomst, obehörig eller oavsiktlig förändring och/eller störning vid databehandling.
- Kommunikationssäkerhet
  Säkerhet i samband med överföring av data, det vill säga åtgärder för att förhindra att känslig information kommer obehörig till del, information förvanskas under överföring, information inte når avsedd mottagare eller blir fördröjd.

IT och digitaliseringfunktionen ansvarar för all it-säkerhet, se kapitel *309.1 - It-säkerhet*.

Information som tillgång

Utifrån policy, riktlinjer, lagar och andra krav ses all registrerad information i Region Halland som viktiga tillgångar och värderas utifrån ett klassningssystem. Varje typ av information som till exempel patienthandlingar, personalhandlingar, ekonomihandlingar får egna värden i form av en säkerhetsnivå. Vilken säkerhetsnivå beror på hur känslig informationen är och vilka risker eller konskevenser det finns om informationen inte hanteras på rätt sätt. Det finns tre säkerhetsnivåer:

- Grundnivå = Lindriga risker/konsekvenser
- Hög nivå = Allvarliga risker/konsekvenser
- Mycket hög nivå = Mycket allvarliga risker/konsekvenser

Mer om informationsklassning, vilka handlingar och olika handlingars säkerhetsnivåer finns i kapitel 107 – *Information, informationsklassning och säkerhetsnivåer*.

Informationskvalitet
Kvaliteten på själva informationen är viktig för att få rätt resultat i verksamheten och för att säkerställa att informationen kan tolkas på ett begripligt sätt och i sitt rätta sammanhang även lång tid efter att den skapades.

Informationskvalitet innebär att informationen är: korrekt, komplett, registrerad/rapporterad i rätt tid, tillförlitlig, noggrann, har rätt detaljeringsgrad och inte är motstridig. Den ska vara försedd med relevant metadata för att kunna tolkas i sitt rätta sammanhang och för att kunna äktheten ska kunna fastställas. Informationskvalitet är en del i hantering av information.

Några principer för att uppnå informationskvalitet:

- Rätt från början (genom utbildning, manualer, valideringar av indata).
- Rätta vid källan.
- Rätta så fort som möjligt, innan en ny information skapas baserad på den felaktiga. Återanvänd redan registrerad information för att minska onödig registrering och undvika registrering av motstridiga uppgifter.

Andra viktiga begrepp för säker informationshantering är:

- Tillgänglighet
  Informationen ska vara tillgänglig för behöriga användare för att personalen ska ha tillgång till information i rätt tid, när den behövs.
- Konfidentialitet
  Informationen ska vara skyddad för obehöriga för att värna om integritet (patienters, medarbetares, leverantörers med flera).
- Riktighet
  Informationen ska vara korrekt och oförvanskad. Den får inte förändras av någon obehörig, av misstag eller på grund av funktionsbrist. Personalen ska ha rätt information för att kunna göra riktiga och säkra bedömningar.
- Spårbarhet
  Informationen ska kunna spåras till enskild användare för att ledningen ska kunna följa upp vem som har gjort vad, var och när i ett it-system.

Dataskydd och hantering av personuppgifter

Personuppgiftsansvar

Personuppgiftsansvarig i offentlig verksamhet är alltid en styrelse eller nämnd. Dessa är ytterst ansvariga för all behandling av personuppgifter inom sina nämnds- eller styrelseområden. Ibland kan också personuppgiftsansvaret vara delat med annan/andra nämnder/styrelser. Regionen hanterar till stor del personuppgifter i sökbara register och kräver en särskild hantering som styrs av Dataskyddsförordningen. Läs mer på Dataskyddsenhetens intranätsida.

Dataskyddsombud (DSO)

Dataskyddsombudet är Regionstyrelsens och driftnämndernas utsedda person som ska kontrollera att dataskyddsförordningen följs. DSO-ombudet ska registreras hos Integritetsskyddsmyndigheten (IMY). Läs mer på IMY:s webbplats.

Dataskyddssamordnare (DSS)

Dataskyddssamordnarna är en stödfunktion som stöttar verksamhet och personuppgiftsansvarig så att personuppgifter behandlas på ett lagligt och korrekt sätt.

Personuppgiftsbiträdesavtal (PUB-avtal)
När någon (t ex leverantör, privata vårdgivare) utanför Region Halland har tillgång till eller behandlar personuppgifter, som Region Halland är personuppgiftsansvarig för, ska ett PUB-avtal upprättas. Se rutin *Personuppgiftsbiträde - upprätta avtal*.

Medarbetares personuppgifter
Region Halland behandlar medarbetares personuppgifter. I rutinen *Personuppgifter - information till dig som medarbetare* finns mer information om dess rättigheter.

Skyddade personuppgifter
Personer som är utsatta för ett allvarligt och konkret hot kan ansöka och få sina personuppgifter skyddade hos Skattemyndigheten. Region Halland ska i all sin verksamhet och system säkerställa att skyddade personuppgifter hanteras på ett korrekt sätt.

Läs mer i rutinerna: *Sekretess i folkbokföringen* och *Offentlighetsprincipen.*

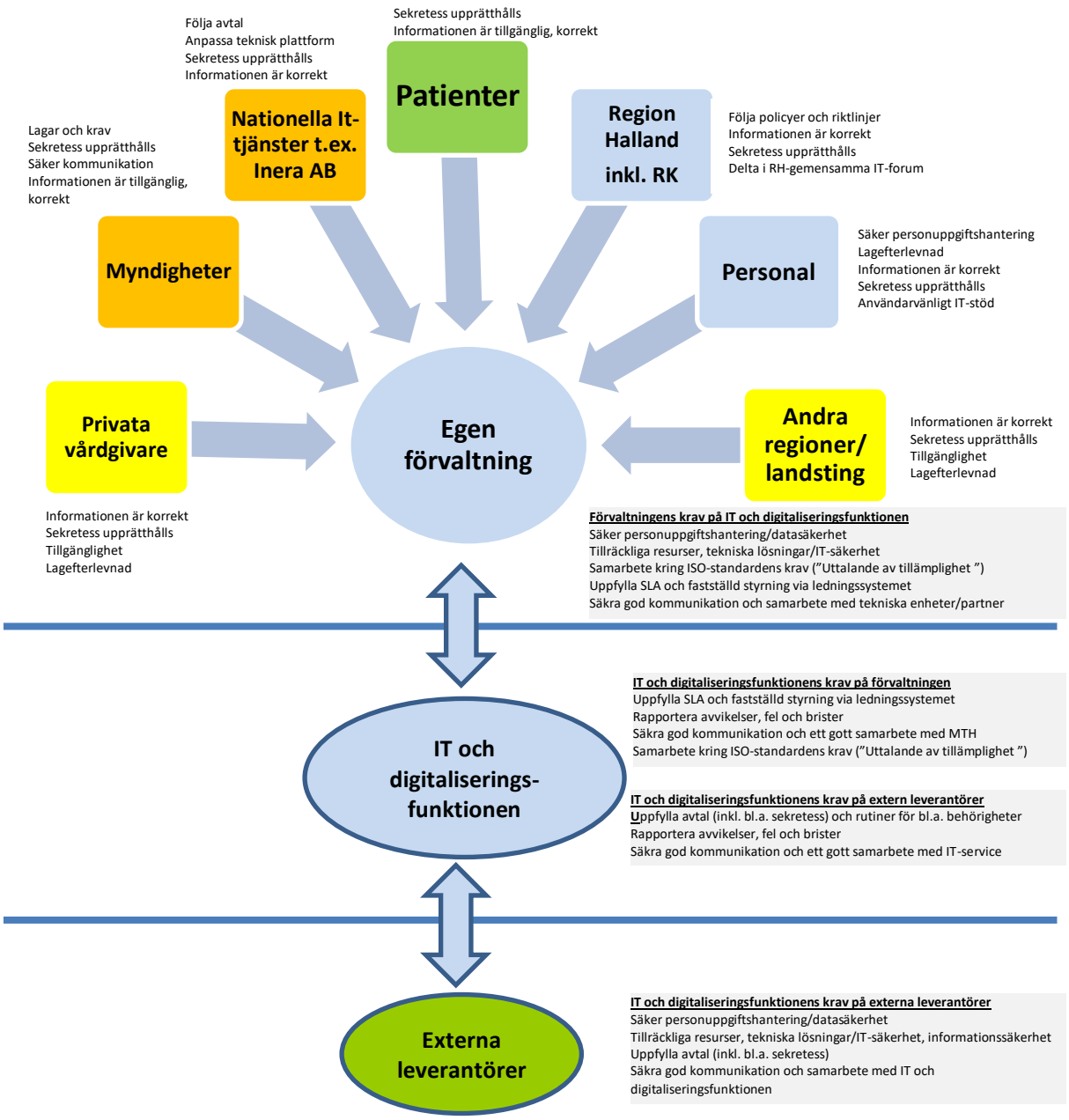
Informationsägare
Informationsägarskapet följer verksamhetsansvaret. Förvaltningschef och verksamhetschef (eller motsvarande) är informationsägare inom sina verksamhetsområden och ansvarar för all hantering av sin verksamhetsinformation. Ansvaret innebär att informationen är:

- är möjlig att nå inom rätt tid (tillgänglighet)
- korrekt (riktighet)
- har rätt spridning (konfidentialitet)

Informationsägarskapet fördelar sig generellt sett på följande vis:
Gemensamma administrativa personregister - förvaltningschef
Vårdsystem och vårdregister – områdeschef, verksamhetschef eller motsvarande
Lokala system och register – avdelningschef eller motsvarande

Verksamhetschef/motsvarande enligt ovan anmäler register till styrelsens/nämndens personuppgiftsombud eller direkt till styrelse/nämnd om ombud saknas.
Se blankett *Personuppgiftsregister - anmälan*. Mer information om hur personuppgifter får behandlas finns i rutin *Personuppgifter - behandling av*.

Gränssnitt för informationssäkerhet



Hantering av information

Följande tabeller visar hur informationen vare sig den är elektronisk, på papper eller på annat medium ska lagras och får kommuniceras.

Lagring av elektronisk information

Lagringsplats	Säkerhetsnivå - Grund	Säkerhetsnivå - Hög	Säkerhetsnivå - Mycket hög
Stationär dator	Inloggningsskydd.	Inloggningsskydd.	Inloggningsskydd. Patientjournaluppgifter får inte lagras.
Bärbar dator	Inloggningsskydd och kryptering.	Inloggningsskydd och kryptering.	Inloggningsskydd och kryptering. Patient-journaluppgifter får inte lagras.
CD, DVD, USB-minne, extern hårddisk, mobila enheter, t ex telefoner, surfplattor.	Surfplattor kräver kod för att låsa upp.	Under direkt uppsikt eller inlåst.	Inlåst. Rekommendation brandsäkert säker-hetsskåp. Patientinfo på cd – en patient per cd märkt med namn och personnummer.
Server i nätverk	Server ska vara inlåst i datorrum med tillträdes-skydd.	Kräver behörighet till information. Server ska vara inlåst i datorrum med tillträdesskydd.	Kräver behörighet till information. Server ska vara inlåst i datorrum med tillträdesskydd.
Säkerhetskopia	Säkerhetskopia i bandrobot får förvaras i dator-serverrum. Övriga inlåsta i brand-klassat utrymme skilt från server- eller datorrum.	Säkerhetskopia i bandrobot får förvaras i dator-serverrum. Övriga inlåsta i brandklassat utrymme skilt från server- eller datorrum.	Säkerhetskopia i bandrobot får förvaras i dator eller serverrum. Övriga inlåsta i brandklassat utrymme skilt från server- eller datorrum.
Återanvänd CD, DVD, USB	Är tillåten.	Är inte tillåten.	Är inte tillåten.
Återanvänd hårddisk	Är inte tillåten.	Är inte tillåten.	Är inte tillåten.
Office 365 - lagring och samarbets-verktyg.	Se rubrik *Arbetsrelaterad information i it-system*	Se rubrik *Arbetsrelaterad information i it-system*	Se rubrik *Arbetsrelaterad information i it-system*
AI verktyg (Copilot)	Se rubrik AI verktyg - Copilot	Se rubrik AI verktyg - Copilot	Se rubrik AI verktyg - Copilot

Elektronisk kommunikation

Elektronisk kommunikation	Säkerhetsnivå - Grund	Säkerhetsnivå - Hög	Säkerhetsnivå - Mycket hög nivå
Inom regionens nät	Får överföras. Tillgänglighet kan styras genom behörigheter och lösenordsskydd.	Får överföras. Tillgänglighet kan styras genom behörigheter och lösenordsskydd.	Får överföras. Tillgänglighet kan styras genom behörigheter till till exempel journal-system, lösenordsskydd.
Externt via regionens nät	Får överföras öppet i nätverk.	RK ITD verkställer kryptering/signering i den mån det är möjligt.	RK ITD verkställer kryptering/signering i den mån det är möjligt.

Elektronisk kommunikation	Säkerhetsnivå - Grund	Säkerhetsnivå - Hög	Säkerhetsnivå - Mycket hög nivå
Uppkopplad förbindelse till regionens nät utifrån	Säker överföring. RK ITD verkställer. Avtal krävs.	Säker överföring. RK ITD verkställer. Avtal krävs.	1) Regelbundna överenskomna förbindelser mellan två parter säkras med kryptering. 2) I övrigt ej tillåtet att skicka elektroniskt.
Trådlöst nätverk	Krypterat.	Krypterat.	Krypterat.
Region Halland Guest (WiFi)	Ja	---	---
Sjunet	--	--	Patientjournaluppgifter får överföras.
Röntgenbilder på CD/DVD	---	---	Till personal med behörighet. Igenklistrat kuvert. Ska skickas med REK.
Röntgenbilder	---	---	1) Regelbundna överenskomna förbindelser mellan två parter säkras med kryptering. 2) I övrigt inte tillåtet att skicka elektroniskt.
Övrig patientinformation	---	---	1) Regelbundna överenskomna förbindelser mellan två parter säkras med kryptering. 2) I övrigt inte tillåtet att skicka elektroniskt.
E-post	Får överföras. Se rutin *E-post*.	Får överföras. Se rutin *E-post*.	Sekretessbelagd information får endast överföras med funktionen *”Säker e-post”*. Se rutin *E-post*.
Trådlös intern Telefoni DECT	--	--	Textmeddelanden är inte tillåtna.
Videokonferens	Får användas.	Får användas.	Får användas under vissa förutsättningar se rutin Videokonferens och chatt.
Rakel	Får användas	Får användas	Får användas
Office 365 - lagring och samarbets-verktyg.	Se rubrik Arbetsrelaterad information i it-system	Se rubrik Arbetsrelaterad information i it-system	Se rubrik Arbetsrelaterad information i it-system
AI verktyg (Copilot)	Se rubrik AI verktyg - Copilot	Se rubrik AI verktyg - Copilot	Se rubrik AI verktyg - Copilot

Lagring/kommunikation av papper, film, band med mera

Hantering	Säkerhetsnivå - Grund	Säkerhetsnivå - Hög	Säkerhetsnivå - Mycket hög
Förvara	Kontors-, arkivlokal.	Kontors-, arkivlokal under direkt uppsikt eller inlåst.	Kontors-, arkivlokal under direkt uppsikt eller inlåst.
Skicka internt (inom RH och privata vårdgivare i Halland)	Inga särskilda krav.	Sekretessprövning i vissa fall. Igenklistrat kuvert i internkuvert. Inte tillräckligt med hophäftat internkuvert. Använd inte förkortningar i adressen.	Sekretessprövning. Igenklistrat kuvert i ett internkuvert eller avsedd plastmapp. Det är inte tillåtet med enbart hophäftat internkuvert. Använd inte förkortningar i adressen. Se rutin *Journalhandling via internpost*.
Skicka externt (utanför RH)	Inga särskilda krav.	Sekretessprövning i vissa fall. Igenklistrat kuvert.	Sekretessprövning. Igenklistrat kuvert med streckkod och rekommenderad försändelse. Se rutin *Journal-utlämnande*. RGS har interna posttransporter till vissa enheter i Halland, VGR och Skåne. Se rutin *Journalhandling via internpost*.
Skicka via fax	Se rutin *Faxöverföring*.	Sekretessprövning i vissa fall. Se rutin *Faxöverföring*.	Sekretessprövning. Se rutin *Faxöverföring*.
Makulera	Inga särskilda krav.	Ska makuleras i dokumentförstörare eller läggas i sekretessbox.	Ska makuleras i dokumentförstörare eller läggas i sekretessbox.
Skanna handlingar - patientjournal	---	---	Patienthandlingar ska skannas in i digitalt journalsystem. Pappersoriginal får gallras efter kontrolläsning och signering.
Inskrivna handlingar - patientjournal	---	---	Patienthandling upprättad i RH får gallras efter inskrivning, kontrolläsning och signering i journal. Patienthandling upprättad av **annan** vårdgivare än RH ska sparas i 3 år efter inskrivning och signering.
Fakturor- skanna handlingar	Faktura ska skannas in i digitalt fakturasystem.	---	Patient- och sekretessuppgifter får inte skannas. Ska hanteras via originalfaktura.
Skanna övriga handlingar	Inga särskilda krav	---	---

Hantering	Säkerhetsnivå - Grund	Säkerhetsnivå - Hög	Säkerhetsnivå - Mycket hög

Förstöring av elektronisk media

Hantering	Säkerhetsnivå - Grund	Säkerhetsnivå - Hög	Säkerhetsnivå – Mycket hög
Förstöring av CD, DVD, USB-minne, diskett, hårddisk etcetera	Hårddisk lämnas till RK ITD, övriga förstörs på lämpligt sätt.	Hårddisk lämnas till RK ITD, övriga förstörs på lämpligt sätt.	Hårddisk lämnas till RK ITD, övriga förstörs på lämpligt sätt. CD och DVD-skivor bryts isär. Minneskretsar bryts eller klipps isär med tång.
Förstöring av hårddisk/minne i medicinteknisk produkt	----	----	Hanteras enligt rutin på MTH.
Förstöring av hårddisk/minne i kopiator och skrivare	Hårddisk lämnas till leverantör.	Hårddisk lämnas till leverantör.	Hårddisk lämnas till leverantör.

AI verktyg - Copilot
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.

Destruering av sekretesspapper.
Sekretesspapper är papper med information som ska vara skyddad för obehöriga. Var god se rutin för krav och metod: Destruering av sekretessinformation

Behov av att öppna sekretesstunna
Om verksamheten har behov av att kunna öppna en sekretesstunna, då de av misstag har slängt något, (viktiga papper, nycklar, telefon) kontaktas Säkerhetsavdelningens funktionsbrevlåda Säkerhetsavdelningen som tar kontakt med Securitas. Securitasväktare får information om vad som har slängts och kommer och låser upp tunnan enligt överenskommelse. Koden lämnas aldrig ut till verksamheten. Verksamheten själv står för utryckningskostnaden.

Destruering av film, band, CD, DVD och disketter
Film, band, CD, DVD och disketter innehållande sekretessinformation läggs i speciell påse avsedd för ändamålet, påsen lämnas till vaktmästarna.
Se rutin: *Avfall, källsorterat* och *Kassering av utrustning/inventarier*.

Allmänna sekretesshandlingar
Allmänna handlingar som registrerats hos en myndighet (nämnd) med sekretessmarkering och som av någon anledning behöver sändas över till annan myndighet (nämnd) ska överflyttas inom Ärendehanteringssystemet Platina.

Fysisk transportering av handlingar
Om bud eller transportfirma ska anlitas bör avtal skrivas med den firma som ska utföra uppgiften. Emballaget måste vara tillräckligt. Om det rör särskilt känslig eller kritisk information ska avtal tecknas och säkerhetsnivån höjas. Åtgärder kan till exempel vara låsta transportbehållare, personligt överlämnande etc.

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

Inköp och upphandling

Vid inköp av vårdrelaterade it-system ska ett antal informationssäkerhetskrav beaktas. Se grunddokument 305 och *Inköp av varor och tjänster – bilaga Informationssäkerhetskrav vid upphandling av vårdrelaterade it-system*.

Sekretess och samtycken

Rutinen *Sekretess och samtycken* beskriver sekretess och när samtycke måste lämnas av patienten. Varje medarbetare har ansvar för att skydda informationen så att obehöriga inte får åtkomst.

Behörigheter och åtkomst till information

Beslut och tilldelning av behörigheter till it-system
Förvaltningschef/verksamhetschef (motsvarande) är informationsägare och beslutar om och tilldelar behörigheter. Detta gäller nyanställda, studerande, vid förändrade uppdrag eller arbetsuppgifter eller vid frånvaro, avslutad anställning etcetera. Använd digital beställning via it-stödet Virgam, i de fall det är möjligt. För övriga beställningar används:

- Rutin: *Behörigheter och åtkomst till it-system*
- Blankett: *Behörigheter it-system*

Gruppinloggning
Strävan är att medarbetare i Region Halland alltid ska identifiera sig i våra IT-system med SITHS-kort och stark autenticering. Gruppinloggning avviker från denna målsättning. Gruppinloggning innebär att flera personer gemensamt använder en inloggningsidentitet.

Gruppinloggning ska så långt som möjligt undvikas då det innebär att bland annat att kravet på stark autenticering och spårbarhet i PDL (vem som gör och läser vad) inte uppfylls. Gruppinloggningskonton ökar också risken för angrepp på vår it-miljö.

Gruppinloggning får endast undantagsvis tillämpas på de ställen där en dator behöver användas av flera personer. Arbetsuppgiften ska vara verksamhetskritisk och inte kunna lösas med personlig inloggning, utan att allvarligt hindra arbetet. Ett gruppinloggningskonto ska ha så liten tillgång som möjligt till it-system med känslig information. Var och en som loggar in ansvarar för sina egna aktiviteter.

Gruppinloggning kan beviljas av IT-säkerhetsansvarig inom RK ITD. Riskanalys ska genomföras innan gruppinloggningsbehörighet tilldelas. Kompletterande säkerhetsåtgärder ska beslutas och införas, som kompenserar för den sänkta säkerhetsnivån.

SITHS-kortet
SITHS-kortet är ett personligt id-kort med elektroniska certifikat som möjliggör säker identifiering av användaren och säker hantering av känslig information. Kort och PIN-koder måste hållas åtskilda. SITHS-kortet får inte lånas ut till någon annan. Om kortet förloras ska det polisanmälas. Se rutiner som börjar med SITHS i ledningssystemet.

In- och utloggning till och från regionens nätverk (RHWLAN)
Användare ska logga in på nätverket med egen inloggningsidentitet (användarnamn och lösenord) alternativt med SITHS-kort. Ett användarnamn kan inte ändras. Identiteten och de resurser som hör till den är personliga. Det är inte tillåtet att låna ut identiteten till någon annan. Den som äger identiteten ansvarar för de aktiviteter som görs.

Lösenord
Lösenordet ska skapas och hanteras enligt rutinen *Lösenord_RH*.

Lämna datorn tillfälligt
När datorn lämnas utan uppsikt ska den alltid låsas. Snabbkommandot är [Ctrl]+[Alt]+[Delete] och därefter [Enter]. Du kan ofta även använda [Win]+[L].

Efter avslutat arbetspass
Städa datorns skrivbord. Dokument sparade på skrivbordet blir inte säkerhetskopierade. Lagring av dokument ska därför göras i avsedda kataloger, enligt förvaltningens dokumenthanteringsplan.

Logga ut dig efter avslutat arbetspass, men stäng inte av datorn. På så sätt får datorn nödvändiga säkerhetsuppdateringar och du blir mindre störd i ditt arbete.

En arbetsplats ska lämnas städad från pappersdokument och andra media, till exempel USB-minnen och CD, som innehåller känslig information. Dessa ska låsas in.

Distansarbete
Med distansarbete avses arbete som utförs regelmässigt en eller flera dagar per vecka eller månad av anställd på arbetsplats som är utanför Region Halland. Distansarbete ska regleras i avtal mellan närmaste chef och medarbetare.
Mer information finns i rutin *Distansarbete - informationssäkerhet*

Distansarbetsplats förutsätter att närmaste chef kan följa upp att arbetet genomförs med samma effektivitet, säkerhet och till samma kvalitet som om arbetet utförts på huvudarbetsplatsen.

Chef beslutar om behörighet till distansåtkomst till regionens nät och beställer funktion hos RK ITD via Intranätet/Stöd och service. Blankett *Behörigheter it-system* ska användas. RK ITD väljer lämplig säkerhetslösning.

Fasta och bärbara datorer som används för distansarbete ska:

- förvaras på ett betryggande sätt
- användas i tjänsten

- endast innehålla program som installerats av RK ITD
- säkerhetskopieras enligt rutin på RK ITD
- lämnas tillbaka när hemarbetet eller anställningen upphör

Medarbetare som vid enstaka tillfällen får löfte om att arbeta hemma, för att exempelvis förbereda sig inför något speciellt, inläsning av material omfattas inte. När det ingår i medarbetares ordinarie tjänst att arbeta på olika geografiska platser inom regionen betraktas inte det som distansarbete.

Extern åtkomst till intranätet
Skriv in adressen https://intra.regionhalland.se i din webbläsare.
Ange användarnamn och lösenord.

E-post via internet
För åtkomst av e-post utanför regionens nät används Outlook Web App.
Skriv adressen epost.regionhalland.se.

SharePoint via internet
Skriv in specifik SharePoint-adress i din webbläsare.
Ange LTHALLAND\ före ditt användarnamn och lösenord.

Loggning - spårbarhet

För att uppnå spårbarhet används loggning och versionshantering. När information skapas, ändras och läses ska detta vara möjligt att spåra. Syftet är att kunna utreda vem som har gjort vad och när då det måste styrkas i till exempel en utredning och för övervakning av åtkomstkontroll. Spårbarhet är lagkrav när det gäller journaldokumentation.

Ansvar
Verksamhetschef ansvarar för att kontroll av loggar i journalsystem genomförs. Den som har rätt att dela ut behörigheter har också skyldighet att granska loggarna. Chef beslutar om vem/vilka som ska ha särskild behörighet (loggkontrollroll) för att ta fram loggunderlag. Chef granskar och signerar genomförd loggkontroll på avsedd blankett.

Se rutin: *Loggkontroll patientjournalsystem*.

Loggning

- Loggen ska visa en obruten lista över händelser i ett system eller i en process under minst ett dygn för vart och ett av de system som används.
- Loggen ska innehålla loggposter för enskilda händelser vilka var och en innehåller information om händelsen, vem som initierade den, när den inträffade med mera.
- Loggen ska inte kunna justeras.
- Läsning och avställning av inaktuella delar av loggen ska vara spårbara.
- Alla aktiviteter som rör juridisk behörighet ska loggas.
- Loggen ska vara läsbar och innehålla uppgifter där det ska framgå vem som är användare, användares arbetsplats, tidsintervall för händelse och vilka aktiviteter som användare utfört.
- Loggen ska utan förändringar kunna exporteras till annan media.
- Loggningsresurser och logginformation ska skyddas mot manipulering och obehörig åtkomst.

- Gallring av data i logg beslutas av respektive nämnd/styrelse i samråd med regionarkivarien. Särskilda regler gäller för patientjournalen.
- Systemadministratörers och systemoperatörers aktiviteter ska kunna följas i en logg.
- Alla inloggades aktiviteter ska kunna följas i en logg.

Uppgifter som loggas
Vad som loggas skiljer sig från system till system. Generellt sett är det följande uppgifter:

- Journalloggar: Användarnamn, arbetsplats, var i journalen, vad användaren gjort, datum, start- och stopptid.
- Internetloggar: IP-nummer, användarnamn, arbetsplats, internetadress, vilken sida som besökts, datum och tid.
- Passerkortsloggar: Efternamn, förnamn, arbetsplats, ingång, datum, klockslag, port.
- Administrativa loggar: Användarnamn, datum, start- och stopptid, var i systemet.
- Systemadministratörsloggar: Användarnamn, datum, start- och stopptid, var i systemet.
- E-postloggar: Användar- och mottagarnamn, arbetsplats, e-postadresser, datum, klockslag, ärenderubrik.

Loggövervakning och logguppföljning internet
System för automatiserad kontroll av internetloggar finns. Internettrafiken kan i realtid (just nu) visas per webbsida. För att nå vissa sidor måste man göra ett aktivt val som loggas. Personal med särskild behörighet på RK ITD övervakar och analyserar vid behov. Verksamhetschef beställer logguppföljning via Servicedesk plus. Arbetsrättsliga åtgärder kan vidtas för användare som missbrukar den begränsade privata användningen med hjälp av regionens it-lösningar.
Se rutin *Internet för personal*.

Logginformation till medarbetare
Chef ansvarar för att informera sina medarbetare om att deras aktiviteter i it-system loggas.
Se rutin *Personuppgifter - information till dig som medarbetare*.

Behörig och obehörig åtkomst till patientjournalen
I rutin *Behörig och obehörig åtkomst till patientjournalen* finns information om när det är tillåtet och inte tillåtet att ta del av innehållet i patientjournal.

Dataintrång, brott mot tystnadsplikt och/eller sabotage it-system
Dataintrång, brott mot tystnadsplikt och/eller sabotage it-system kan leda till arbetsrättsliga åtgärder eller polisanmälan.
Se rutin *Dataintrång, brott mot tystnadsplikt och/eller sabotage it-system, misstanke om*.

Utlämnande av handling

Vid begäran om utlämnande av allmän handling ska bedömning av eventuell sekretess alltid göras, se rutin *Offentlighetsprincipen – introduktion*

Begäran om loggutdrag från journal
Ett loggutdrag är en allmän handling som ska lämnas ut efter sekretessprövning enligt offentlighets- och sekretesslagen.
Se rutin *Loggutdrag till patient*.

Begäran om e-post och e-postloggar
Verksamhetschef/avdelningschef/motsvarande, där den loggade personen är anställd eller har ett uppdrag samt registrator på Regionkontoret får beställa utdrag av e-postloggar hos RK ITD. En beställning ska göras i ärendesystemet SD+. RK ITD ska genomföra beställningen skyndsamt. Utdraget skickas från RK ITD till beställaren med e-post. Det är beställaren som sekretessprövar loggutdraget innan utlämnande till den som begärt.

Vid en begäran om utlämnade av specifikt e-postmeddelande hanteras begäran företrädelsevis inom den berörda verksamheten. Före utlämnandet ska e-postmeddelandena sekretessprövas. För hjälp med beslut om ett utlämnande ska göras kan chef ta kontakt med regionjurist. Se rutin: E-post

Datorer och annan utrustning

Det är förbjudet att ansluta datorer, som inte ställts i ordning av RK ITD till regionens nät. Datorn kan upplevas som personlig, men den är precis som övrig utrustning ett redskap i arbetet.

Installation av system och programvara
För att säkerställa att det inte av misstag eller medvetet installeras programvara som kan ha skadlig påverkan på systemmiljö eller andra informationskällor kan och får inte användare installera programvara. För att kunna göra detta krävs uppdrag och behörighet motsvarande administratörsbehörigheter.

Behov av att installera programvara eller tillägg till programvara lämnas till närmaste chef som tar upp det enligt systemförvaltningsmodellen.

Mobil datoranvändning
För trådlös kommunikation med bärbar dator, handdator, surfplatta eller mobiltelefon gäller samma säkerhetskrav som för all annan informationshantering med datorer.
Användare av mobil datorutrustning har ett personligt ansvar för utrustningen och ska vara aktsamma och skydda utrustningen så att obehöriga inte får tillgång till den eller insyn i den – skärmlås med PIN-kod eller fingeravtryck ska vara aktiverat.

Bärbar dator eller motsvarande utrustning får inte lämnas obevakad på allmän plats. Vid resa ska den medföras som handbagage. Den ska vara stöldmärkt och den ska vara försedd med regionens antivirusskydd. Känslig information på bärbar dator ska vara krypterad.
Arbete med känsliga personuppgifter på allmän plats, till exempel caféer, väntsalar eller tåg är inte tillåtet. Under förflyttning mellan arbetsplatsen och hemmet eller annan plats ska medarbetaren vara utloggad, datorn ska vara avstängd och förvaras i datorväska. I hemmet ska datorn placeras i avskilt rum, där inte obehöriga vistas. När datorn lämnas utan uppsikt ska den låsas med hjälp av [Ctrl]+[Alt]+[Delete] därefter [Enter] även [Win]+[L] fungerar oftast.

Inaktivering av datorer
För att säkerställa att datorer har en tillfredsställande säkerhetsnivå avseende antivirus och uppdateringar har Tjänsten IT-säkerhet mandat att inaktivera bärbara datorer när de varit inaktiva/avstängda i nätverket under mer än tre månader. För stationära datorer är tidsgränsen en (1) månad.

Förteckning
RK ITD för förteckning över samtliga verksamheters it-utrustning (datorer, skrivare med mera) och it-system.

Kassering/Återanvändning
Se Rutin *Kassering av utrustning/inventarier*.

Mobiltelefon

Mobiltelefon är oftast inte bara en telefon. Den kan ha flera funktioner som till exempel bokningskalender, möjlighet att ta emot och lagra e-post och bilder, skriva och lagra anteckningar och fotografera.

Ingen känslig information får skickas eller lagras i en mobiltelefon. Kameran får inte användas i patientrelaterat arbete. På platser där det är förbjudet att använda mobiltelefon ska detta respekteras. Du måste lägga in ett personligt lösenord för inloggning.

Synkronisering
Det är praktiskt att ha tjänstemobilen synkroniserad till Outlook/Exchange, men innan synkronisering sker ska man vara medveten om att synkronisering också innebär att RK ITD får rättigheter att i Outlook/Exchange tömma hela telefonen på innehåll inklusive att radera minneskort om problem uppstår. Funktionen är bra att ha när man förlorat sin telefon. Detta måste godkännas i inställningarna när kontot läggs in.

Utomlands
När tjänstemobilen är synkroniserad till Outlook/Exchange finns en del att tänka på inför utlandsvistelser. Mobilabonnemangen är inte spärrade för samtal eller datatrafik i utlandet. När en mobilabonnent lämnar Sverige och radiotäckningen från dess ordinarie teleoperatör upphör, växlar telefonen över till en teleoperatör i det besökta landet, så kallad roaming. Det kan ske helt automatiskt utan att du märker det. Det är därför viktigt att stänga av roamingen för att inte debiteras enorma extra kostnader. Stäng av Mobilt nätverk helt. Surfa därför inte mer än nödvändigt. Hur du avaktiverar synkroniseringen till Outlook/Exchange finns i guider på Intranätet/Stöd och service/Självservice/Telefoni.
Vid utlandsvistelse debiteras du för alla samtal som ringer till din telefon. Den som ringer till dig betalar för samtalet inom Sveriges gräns som vanligt, men all överskjutande kostnad debiteras på mottagarens telefon.

Förlust
Vid förlust av tjänstemobilen kan du själv ta bort synkroniseringen och informationen via https://epost.regionhalland.se. Du kan också kontakta din HAK-administratör eller Teleservice.
Vid stöld ska SIM-kortet omedelbart spärras. Ta kontakt med Servicedesk telefoni.
Se förvaltningens rutin *Mobiltelefon* och regiongemensam rutin *Externa lagringsmedia*.

Lagring av information

Information, som lagras i filserverkataloger eller i it-system, är arbetsmaterial. Den ska kunna gallras efter en kortare tid. Information som inkommer till myndigheten eller som upprättas i slutgiltig form och/eller skickas från myndigheten utgör allmänna handlingar. Dessa allmänna handlingar ska registreras i myndighetens diarium eller ska de hållas ordnade så att det utan problem ska gå att se om de inkommit till myndigheten eller upprättats där, så kallad

systematisk förvaring. Systematisk förvaring lämpar sig för information som har en naturlig inbördes ordning, t.ex. kronologisk eller alfabetisk.

Arbetsrelaterad information och privat användning av it-system
Informationen i våra it-system, på flyttbara lagringsenheter och i mobila enheter tillhör Region Halland och ska vara arbetsrelaterad.

Patientuppgifter
Patientuppgifter inklusive foton får endast sparas i särskilda vårdsystem eller i undantagsfall (digitala bilder) på cd. Se under rubrik *Lagring av elektronisk information*.

Privat användning
Medarbetare som lagrar och delar upphovsrättsskyddat material (exempelvis fildelning av musik eller filmer) gör sig skyldiga till lagbrott. Onödig lagring belastar också Region Hallands systemresurser och drabbar verksamheten när prestanda försämras. Att använda regionens lagringsutrymmen för privat bruk kan leda till arbetsrättsliga åtgärder.

Lagringsplatser
All lagring av dokument ska göras i avsedda verksamhetssystem eller kataloger enligt förvaltningarnas dokumenthanteringsplaner.

Datorns skrivbord
Ingen information ska sparas på datorns skrivbord. Denna yta säkerhetskopieras inte.

C:-katalog
Lokal hårddisk på datorn som inte heller ska inte användas för lagring av dokument. Säkerhetskopieras inte.

G:-katalog (Katalogen kommer att tas bort. Fortsatt användning utgör undantag)
Här sparas verksamhetsgemensamma dokument (ej patientuppgifter).

I:-katalog
I-katalogen är endast tillåten för forskning. (en personuppgiftsregisteranmälan ska först göras). Behörigheter till respektive mapp ska vara strikt begränsad och ska avslutas när forskningsuppdrag upphör.

På I:-katalogen kan även program som innehåller patientdata finnas. Verksamhetschef beställer behörighet till programmapp. Behörigheter till respektive programmapp ska vara strikt begränsat och avslutas så snart programmet avvecklats.

Y:-katalog
Här sparas förvaltningsgemensamma dokument från exempelvis arbetsgrupper som arbetar över klinik/avdelningsgränserna. Administreras av personal med särskild behörighet.

Teams och SharePoint Online
I Teams och SharePoint online kan information lagras, som behöver delas av flera. Det handlar om deltagare i projekt, ledningsgrupper, nätverksgrupper etcetera.

Chefen ansvarar för behörighetstilldelning. Tilldelning ska ske med samma restriktivitet som vid all annan behörighetshantering. Behörighet ska tas bort när medarbetaren byter arbetsuppgift eller slutar sin anställning.

Medarbetaren ansvarar för den information som lagras. Medarbetaren ska veta att informationen får lagras i Teams samt se till att den är korrekt och att den raderas när den inte är aktuell. Då det är väldigt enkelt, att med hjälp av Teams, dela information är det viktigt att medarbetaren tar ansvar för att information inte delas med personer som är obehöriga.

Medarbetaren ansvarar också för att informationen förs över till annan medarbetare vid anställningens avslut eller byte av arbetsuppgifter. Finns ingen tydlig mottagare ska informationen istället hanteras av chefen.

Inaktiva Teams ska avvecklas och informationen ska antingen raderas eller tas om hand.

Lagring och radering ska alltid följa förvaltningens dokumenthanteringsplan. Teams är inget diariesystem eller arkivsystem. Handlingar som ska diarieföras ska överföras till Platina.

Det är alltid innehållet i filerna som styr vad som är tillåtet och vad som inte är tillåtet att hantera i Teams och SharePoint.

Exempel: En faktura innehåller känsliga uppgifter om den riktar sig till en patient, det vill säga patientuppgifter, och får inte hanteras i Teams och SharePoint. En faktura utan patientuppgifter är enbart att betrakta som harmlös och är tillåtet.

Nedan presenteras ett antal exempel på information som vanligtvis är tillåtet och inte tillåtet att hantera.

Tillåtet
- Rutiner, blanketter, manualer, utbildningsbildspel, schema, mötesanteckningar, arbetsdokument, presentationer, utbildningsbildspel, avtal.
- Riskanalyser och revisionsrapporter som inte är av känslig karaktär (det vill säga som inte omfattas av Offentlighets- och sekretesslag (2009:400)).
- Personuppgifter som inte är känsliga, exempelvis namn, adress, personnummer mm.

Inte tillåtet
Se rubrik: OneDrive

OneDrive
Här sparas dokument som användaren bara själv kommer åt men det är även möjligt dela mappar och filer med andra. Vad alltid extra försiktig när du delar ut åtkomst till dina filer så att inte fel personer får åtkomst. Vid länkdelning till personer utanför Region Halland ska *tidsbegränsning* aktiveras. Tidsbegränsningen ska sättas så snävt som möjligt.

Alla säkerhetsnivåer enligt regionens informationsklassningsmodell (grund, hög och mycket hög) får lagras på OneDrive såvida uppgifterna inte innehåller sekretess eller är personuppgifter som är att betrakta som känsliga eller skyddade.

På OneDrive är det ***inte*** tillåtet att lagra
- Sekretess enligt Offentlighets- och sekretesslag (2009:400), exempelvis:
    - Hälso- och sjukvårdssekretess (25 kap)
    - Upphandlingssekretess (19 kap. 1 §, 31 kap. 3 § och 16 §)
    - Risk och sårbarhetssekretess (18 kap. 13 §)
    - Försvarssekretess (15 kap. 2 §)

- m.fl.

- Känsliga personuppgifter
  - etniskt ursprung
  - politiska åsikter
  - religiös eller filosofisk övertygelse
  - medlemskap i en fackförening
  - hälsa
  - en persons sexualliv eller sexuella läggning
  - genetiska uppgifter
  - biometriska uppgifter som används för att entydigt identifiera en person.

- Skyddade personuppgifter
  - uppgifter om person som skyddas i Skatteverkets folkbokföringsregister.

- Verksamhetskänslig information
  - sådan information som verksamheten bedömer behöver ett extra skydd

Det finns inget som hindrar att man lagrar information med ett högre skydd, men den får aldrig lagras med för lågt skydd. Det kan alltså vara bättre att lagra i Platina än OneDrive, om man är osäker på skyddsbehovet. Verksamhetskänslig information kan motivera en höjd skyddsnivå. Exempel på sådan information kan vara IT-systemdokumentation eller incidenthanteringsinformation, som skulle kunna nyttjas av en angripare. Ett annat skäl kan vara att man vill hålla samman likartad information med olika högt skyddsbehov.

Intranätet
På intranätet lagras information och styrda dokument som ska vara tillgängliga för flera. Särskilda behörigheter krävs. På samarbetsplatserna får inga patientuppgifter lagras.

Biblioteks- och mappstruktur samt olika Teams
En biblioteks- och mappstruktur ska vara tydlig och överskådlig, så att information lätt kan både lagras och hämtas. Ett bibliotek består av mappar på olika nivåer och antalet nivåer bör begränsas. Biblioteksstrukturen ska vara uppbyggd utifrån hur verksamheten är organiserad, det vill säga arbetsområde och ämne.

Ledningens kontroll
Ledningen har rätt att få inblick i och kontrollera all information som är lagrad i regionens it-system. Ledningen kan därför när som helst kontrollera vad som finns lagrat i regionens lagringsutrymmen. Hanteringen ska ske i vittnes närvaro. Använd blankett *Inloggningsuppgifter - beslut om nollställning*

Kommunikation

Verksamheter som tillåts skapa och driva egna hemsidor på www.regionhalland.se ska följa kommunikationsavdelningens rekommendationer för webbproduktioner. Kommunikationsavdelningen ansvarar för innehållet på regiongemensamma sidor.
Se rutin *Domännamn*.

Sociala medier
Se rutin för Sociala medier.

I specifika fall kan chef besluta om att Facebook-konto får användas i tjänsten, till exempel vid projektarbete, studier i tjänsten under begränsad tid.

Videokonferens och chatt
Videokonferens får under vissa förutsättningar även användas till att utväxla patient- och sekretessbelagda uppgifter. Via funktioner såsom ”dela skrivbord” blir allt som visas på skärmen blir synligt, till exempel journaluppgifter och *måste användas med stor försiktighet!* Läs mer i rutin *Videokonferens och chatt*.

Incidenthantering och avvikelser

Incidenter
Allvarliga informationssäkerhetsincidenter ska anmälas omgående till:
Servicedesk 010-47 61 900.

Exempel på allvarliga informationssäkerhetsincidenter är misstanke om skadlig kod, dataintrång, förlust av inloggningsuppgifter, förlust av dator, läsplatta och mobiltelefon eller om kritiska verksamhetssystem kraschar.

Personuppgiftsincidenter anmäls via webbsidan *Rapportera avvikelse*

Mindre allvarliga incidenter kan anmälas via intranätet: IT och telefoni (regionhalland.se)

Dessutom ska även incidenter registreras i avvikelsesystemet.

Avvikelser
Avvikelser hanteras och registreras i Platina avvikelsesystem. Även incidenter är avvikelser och ska utredas på samma sätt. Det är viktigt att alla avvikande händelser rapporteras så att förbättringsåtgärder kan vidtas.

Förvaltningens informationssäkerhetssamordnare ska informeras om avvikande händelser och kan medverka vid händelseanalyser.

Läs mer Avvikelser och incidenter

Supportärenden till Servicedesk

Ärenden anmäls via intranätet:
IT och telefoni (regionhalland.se), eller
Telefon 010-47 61 900

Datornamn och serienummer som RK ITD behöver visas på varje dators skrivbord. Personuppgifter som har betydelse för ärendet får inte anges i själva ärendetexten utan ska noteras inne i ärendet.

Verksamhetsnära stöd

It-samordnare och it-ombud

- Problem med inloggning, behörighet, lösenord i system.
- Handledning i datoranvändning.
- Allmän support för användarna på arbetsplatsen.
- Kontaktperson gentemot RK ITD.

Mer information om it-samordnare och it-ombud finns på: Intranätet | Stöd och service.

HAK-uppdaterare
När det gäller inloggning på datorn kontakta din HAK-uppdaterare.

IT-hjälpen Tandvård
Vid problem eller behov av support med tandvårdsprogrammen Opus, Dimaxis, Romexis och C-takt anknytning 31 400.
Övriga it-problem ska anmälas till IT och telefoni (regionhalland.se).

Förvaltning av it-system

RK ITD ansvarar för förvaltning av Regionen Hallands IT-system. IT-system kravställs, införs och utvecklas i partnerskap med verksamheten.

Extern personal

Exempel på extern personal: Studenter, konsulter, entreprenörer, politiker, trainee, hyrpersonal, leverantörer, hantverkare och servicepersonal.

Informationssäkerhetskrav
Extern personal (vanligtvis it-konsulter) som behöver tillgång till Region Hallands nätverk och it-system hanteras enligt följande rutin: *Leverantörer och konsulter - behörigheter och anslutningsavtal.* Undertecknade blanketter sparas lämpligtvis i pärm eller i årsakt i diariet.

Extern personal som **inte** ska ha tillgång till regions it-system, exempelvis hantverkare och servicepersonal. Se rutin: *Entreprenörer och konsulter - regler.*

Externa leverantörer och konsulter ska ta del av innehållet i introduktion till informationssäkerhet – extern och undertecknas. Undertecknad sekretesskvittens förvaras på respektive förvaltning i 70 år. *Introduktion till informationssäkerhet - extern*

Behörighetstilldelning
Undertecknad behörighetsblankett sparas hos uppdragsgivaren i 10 år. Gruppinlogg är inte tillåtet för leverantörer och konsulter.
Se rutin: *Leverantörer och konsulter - behörigheter och anslutningsavtal*

SITHS-kort
Hantering av SITHS-kort till extern personal framgår i *Rutin: SITHS - Beställa och återlämna.*

Molntjänstleverantörer
Molntjänster innebär att exempelvis processorkraft, lagring och funktioner tillhandahålls av leverantörer som tillhandahåller tjänster över internet. Att teckna avtal med en molntjänstleverantör är komplext, vilket kräver en noggrann granskning ur informationssäkerhetssynpunkt samt att riskanalys genomförs.
Då det uppstår en situation där en molntjänst kan bli aktuell kontakta alltid IT- och digitalisering samt Dataskyddsenheten. Avtal med molntjänstleverantör får inte tecknas innan det finns beslut på om tjänsten får användas.

Privata vårdgivare

Patientdatalagen medger under vissa förutsättningar att vårdgivare, privata och offentliga kan utbyta patientinformation när man är överens i ett avtal om sammanhållen journal. I vårdavtal mellan Regionstyrelsen och privata vårdgivare som använder VAS finns överenskommelser om sammanhållen journal.

Uppdaterat från föregående version

Uppdaterat information kring destruering av sekretesspapper. Hänvisar till ny rutin Destruering av sekretessinformation

Tidigare versionsuppdateringar

Lagt in information om AI verktyget Copilot

- Kompletterande information om sekretesstunnor
- Förtydligat om ansökan att använda molntjänst

Ersätter 2022-01-11