Region Värmland

Granskning av regionens hantering av skyddade personuppgifter

Building a better working world

Innehållsförteckning

1. Sammanfattning

EY har på uppdrag av regionrevisorerna granskat om styrelse och nämnder säkerställt en tillräcklig intern styrning och kontroll vid hantering av skyddade personuppgifter så att dessa inte riskerar att röjas för obehöriga. Sammantaget görs bedömningen att styrelse och nämnder inte i tillräcklig omfattning säkerställt intern styrning och kontroll.

Det finns ett antal riktlinjer, rutiner och anvisningar för hanteringen av personer med skyddade personuppgifter, inklusive medarbetare. Dessa styrande dokument bedöms i huvudsak vara utförliga och omfattar nödvändiga beskrivningar av hanteringen av personer med skyddade personuppgifter. Det finns dock behov av utförligare regionövergripande och verksamhetsspecifika beskrivningar baserat på inventerade riskmoment. Vissa styrande dokument är utformade på ett sätt som inte motsvarar det stöd som personal efterfrågar. De riktlinjer som tillämpas bör enligt vår mening vara fastställda av regionstyrelse och berörda nämnder, inte som idag av chefsfunktioner, eftersom det kan stå i strid med regionfullmäktiges beslut om att riktlinjer endast i undantagsfall kan antas av chefer.

Det finns risker av allmän karaktär som gäller hela regionen, exempelvis extern kommunikation med myndigheter, ändamålsenliga systemstöd, telefonkontakt med privatpersoner, avvikelsehanteringen, brister i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare samt tydligare rutiner för hanteringen av medarbetare. Vidare finns verksamhetsspecifika risker som är unika för varje situation.

Vi uppmärksammar kompetens och kunskapsspridning som särskilda utvecklingsområden. Medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter bör stärkas genom obligatoriska utbildningar och informationsspridning då mänskliga faktorn identifierats som stor risk i hanteringen av skyddade personuppgifter.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån genomförd risk- och konsekvensanalys. Regionstyrelsen eller granskade nämnder har därmed inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontrollerar att rutinerna efterlevs. Avvikelser systematiseras och aggregeras inte för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter.

Utifrån granskningens iakttagelser rekommenderar vi Regionstyrelsen och granskade nämnder, utifrån sina respektive uppdrag och ansvarsområden, att tillse att det:

- Genomförs risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov lyfta in bedömda risker i internkontrollplanerna.
- Genomförs en översyn av de styrande dokumentens klassificering och beslutshierarki avseende skyddade personuppgifter i syfte att säkerställa så regionstyrelse och nämnder fastställer riktlinjerna.
- Genomförs obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument avseende skyddade personuppgifter samt avvikelsehantering, erfarenhetsanalys och i praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.
- Övervägs att inrätta ”compliancefunktion/-er”, det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp. Detta för att hanteringen av skyddade personuppgifter ska vara prioriterat i regionens verksamheter.
- Genomförs penetrationstester av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång.
- Genomförs systematiska loggkontroller i samtliga systemstöd i syfte att säkerställa att obehöriga inte kan få tillgång till skyddade personuppgifter.
- Sker uppföljning av incidenter och avvikelser samt att avvikelsehanteringen avseende skyddade personuppgifter stärks.

2. Inledning

2.1. Bakgrund

I Revisionsplan 2022 har regionrevisorerna beslutat granska hanteringen av skyddade personuppgifter inom Region Värmland. Det är en angelägen uppgift för samhället att ge skydd till de personer som riskerar att utsättas för olika typer av brott, hot och förföljelse och därav lever med skyddad identitet. I många av regionens verksamheter ingår hantering av personuppgifter, liksom för regionens egen personal. Det är viktigt att säkerställa att skyddade personuppgifter inte röjs då det kan leda till allvarliga konsekvenser för den enskilde. Om det skyddade personuppgifter hanteras på felaktigt sätt kan det även leda till att regionen tvingas erlägga skadestånd eller sanktionsavgift.

2.2. Syfte och revisionsfrågor

Syftet är att granska om styrelse och nämnder säkerställt en tillräcklig intern styrning och kontroll när det gäller hantering av skyddade personuppgifter så att dessa uppgifter inte riskerar att röjas för obehöriga.

I granskningen besvaras följande revisionsfrågor:

- Har styrelse och nämnder tillsett att det finns ändamålsenliga rutiner för hantering av skyddade personuppgifter.
- Har styrelse och nämnder säkerställt att det finns tillräcklig kunskap och erforderlig utbildning om gällande regelverk hos den personal som hanterar skyddade personuppgifter inom Region Värmland.
- Har styrelse och nämnder tillsett att det sker en tillräcklig uppföljning och kontroll av att rutinerna efterlevs.
- Har styrelse och nämnder säkerställt att obehöriga inte kan få tillgång till skyddade personuppgifter genom till exempel användande av behörigheter och kontroller i olika datasystem.

2.3. Ansvariga nämnder

Granskningen avser Regionstyrelsen, Hälso- och sjukvårdsnämnden, Kollektivtrafiknämnden, Kultur- och bildningsnämnden, Regionala utvecklingsnämnden samt Patientnämnden.

2.4. Metod och genomförande

Granskningen bygger på dokumentstudier, intervjuer samt stickprov av vårdinformationssystem (patientjournal), avvikelsehantering, loggrapporter, elevregister samt lönelistor. Intervjuer har genomförts med företrädare för berörda verksamheter och med ordföranden i respektive granskad styrelse/nämnd. Intervjuade funktioner och granskade underlag framgår av källförteckning.

I uppdraget ingick att genomföra en större enkät till personal inom regionens verksamheter men efter begäran från verksamhetsföreträdare avbeställdes den. Därmed kan granskningen inte återge ett bredare underlag än via de 34 intervjuer som återger beskrivningar och uppfattningar kring hanteringen av skyddade personuppgifter.

Bedömningar, slutsatser och rekommendationer utgår från den samlade bilden av styrande dokument som inventerats och jämförts med hur representanter för regionens verksamheter i intervjuer beskriver och uppfattar förutsättningarna att hantera skyddade personuppgifter. Denna ansats motiveras av att styrande dokument i sig inte är en garant för ändamålsenliga rutiner där vi definierar ordet ”rutiner” som det sätt på vilket ansvariga i praktiken utför arbetsuppgifterna jämfört med beskrivningar av hur det ska gå till.

Behovet av tillräcklig kunskap och erforderlig utbildning bedöms utifrån hur utbildningsutbudet inom skyddade personuppgifter är upplagt samt intervjuades uppfattningar om kompetensbehov.

Vid bedömning av huruvida styrelse och nämnder tillsett en tillräcklig uppföljning och kontroll av att rutiner efterlevs utgår granskningen från internkontrollprogram och protokoll.

Den sista revisionsfrågan om styrelse och nämnder säkerställt att obehöriga inte kan få tillgång till skyddade personuppgifter besvaras genom intervjuer med intern IT-expertis samt loggrapporter.

Utöver detta har ett selektivt urval av data specifikt avseende skyddade personuppgifter gjorts i patientjournaler, avvikelsehantering, loggrapporter, elevregister samt lönelistor. Syftet har varit att vidimera att uppgifter som lämnats i samband med intervjuer är korrekta.

2.5. Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna utgörs huvudsakligen av:

- Kommunallagen (2017:725)
- Offentlighets- och sekretesslagen (2009:400)
- SFS 2018:684 Lag om ändring i folkbokföringslagen (1991:481)
- Patientdatalagen (2008:355)
- Skatteverket ”Folkbokföring – sekretessmarkerade personuppgifter” samt ”Viktigt för myndigheter att tänka på för att systemet med markering för skyddad folkbokföring och sekretessmarkering ska fungera”
- Av regionfullmäktige antagna styrdokument

Dessa beskrivs närmare i kapitel 2 och 3.

3. Utgångspunkter för granskningen

3.1. Kommunallagen (2017:725)

Regionstyrelsen ska enligt 6 kap. 1 § kommunallagen (KL) leda och samordna förvaltningen av regionens angelägenheter och ha uppsikt över övriga nämnders verksamhet. Av 6 kap. 11 § KL framgår att styrelsen ska följa de frågor som kan inverka på regionens utveckling och ekonomiska ställning.

Av 6 kap. 6 § KL framgår att nämnderna var och en inom sitt område ska se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som beslutats av regionfullmäktige samt de föreskrifter som gäller för verksamheten. Nämnderna ska även tillse att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt.

3.2. Om begreppet skyddade personuppgifter

Det har blivit vanligare att människor lever med skyddade personuppgifter. De senaste tio åren har antalet dubblerats från drygt 12 000 till knappt 24 000 personer. Enligt Skatteverket utgörs dessa till 59 procent av kvinnor. Vanligast förekommande är sekretessmarkering, som är den minst ingripande formen av skydd, med 82 procent av ärendena medan skyddad folkbokföring, som är ett starkare skydd, utgör 18 procent.

Antalet personer med skyddade personuppgifter motsvarar ca 0,22 procent av befolkningen och matematiskt motsvarar det ca 650 invånare och ett tjugotal anställda. Siffrorna är inte exakta men visar att det statistiskt handlar om ett fåtal individer. Konsekvensen vid felaktig röjning av dessa personuppgifter kan emellertid vara mycket allvarlig för var och en.

Jämställdhetsmyndigheten har på regeringsuppdrag genomfört kunskapshöjande insatser gällande våldsutsatta personer som lever med skyddade personuppgifter med fokus på kvinnor och barn. I en delrapport[1] intervjuas 86 kvinnor och 15 barn om deras erfarenheter. Närmare tre fjärdedelar av de intervjuade uppger att deras identitet har röjts.

I rapporten konstateras att det i många fall handlar om kvinnor och barn som tvingats flytta på grund av våld och hot från närstående man och att målgruppen är extra utsatta. I princip samtliga kvinnor i Jämställdhetsmyndighetens intervjustudie har fått skyddade personuppgifter röjda av myndigheter.

3.3. Det finns omfattande lagstiftning som skyddar individen

Skyddade personuppgifter är ett samlingsbegrepp för olika åtgärder som kan vidtas för att skydda personer som riskerar att utsättas för hot, våld eller förföljelse. Beroende på hotets allvarlighetsgrad finns tre grader av skydd av personuppgifter; sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter. Därutöver finns ytterligare bestämmelser om sekretess som kan aktualiseras för hotade och förföljda personer, bland annat inom offentlighets- och sekretesslagen (2009:400).

3.3.1 Sekretessmarkering är den vanligaste och minst ingripande formen av skydd

Sekretessmarkering är den minst ingripande formen av skydd av personuppgifter som innebär att Skatteverket gör en sekretessmarkering av enskild persons uppgifter i folkbokföringen (se 5 kap. 5 § offentlighets- och sekretesslagen [2009:400], OSL). Syftet är att förhindra att hotande eller förföljande person med hjälp av personuppgifter kan hitta och utsätta person för brott, förföljelse eller trakasserier.

Sekretessmarkeringen är dock inte ett bindande beslut, endast en indikation på att folkbokföringssekretess enligt 22 kap. 1 § OSL kan gälla för uppgifterna. Den fungerar alltså som en påminnelse eller varningssignal hos alla myndigheter om att det finns behov att göra en noggrann sekretessprövning innan personuppgifter lämnas ut.

I praktiken registrerar Skatteverket en sekretessmarkering som aviseras tillsammans med personuppgifterna till alla myndigheter som får grundläggande personuppgifter från Skatteverkets folkbokföringsverksamhet. Skatteverket vidareförmedlar post till personer med sekretessmarkering.

[1] *Skyddade personuppgifter – Oskyddade personer* (Rapport 2022:10).

Det är den enskilde som ansöker om sekretessmarkering hos Skatteverket. Det finns inga formella krav för att beviljas skyddsåtgärden men den enskilde behöver motivera varför den behöver sekretessmarkering med någon form av handling eller intyg som stödjer att det föreligger ett aktuellt och konkret hot. Det kan till exempel vara en utredning eller ett utlåtande från Polismyndigheten eller socialtjänsten. Sekretessmarkeringen gäller ofta i två år och kan förlängas.

3.3.2 Skyddad folkbokföring ger starkare skydd än sekretessmarkering

Skyddad folkbokföring ger starkare skydd än sekretessmarkering och innebär att en person kan vara folkbokförd på sin gamla folkbokföringsort efter att ha flyttat. De gamla adressuppgifterna tas bort och den nya adressen registreras inte i folkbokföringen och sprids därmed aldrig till andra myndigheter. Uppgifterna om skyddad folkbokföring skickas till andra myndigheter och annan samhällsservice som personen har kontakt med, till exempel sjukvården, Försäkringskassan och kommunen. Det betyder att dessa instanser kan se att personen har skyddad folkbokföring.

Skyddad folkbokföring medges för person som av särskilda skäl kan antas bli utsatt för brott, förföljelser eller allvarliga trakasserier på annat sätt, om åtgärden med hänsyn till den enskildes förmåga och övriga förutsättningar kan antas tillgodose behovet av skydd. Skyddad folkbokföring kan kombineras med andra skyddsåtgärder som exempelvis kontaktförbud om det bedöms lämpligt utifrån den enskildes specifika situation. Skyddad folkbokföring medges efter ansökan från den enskilde. För barn under 18 år får ansökan göras av enbart en vårdnadshavare om syftet är att skydda från den andra vårdnadshavaren.

3.3.3 Fingerade personuppgifter är den starkaste och mest ingripande formen av skydd

År 2015 fanns i Sverige ungefär 160 personer med fingerade personuppgifter. Omräknat till befolkningsstorlek motsvara det fyra värmlänningar, alltså väldigt få. Fingerade uppgifter betyder att personen använder andra personuppgifter än de verkliga. Detta medför dock inte någon rättslig förändring av personens namn eller andra förhållanden. Kopplingen mellan den verkliga och den fingerade identiteten är sekretessbelagd. Med den nya identiteten kan personen vara öppen med sina personuppgifter utan risk att bli hittad.

Det är den enskilde som ansöker om fingerade personuppgifter hos Polismyndigheten. Medgivandet får begränsas till viss tid. En person som ansöker om, eller fått medgivande att använda fingerade personuppgifter, får ansöka om medgivande även för barn som personen är vårdnadshavare för och varaktigt bor tillsammans med, om syftet är att ge skydd mot den andre vårdnadshavaren.

Myndigheter är skyldiga att lämna upplysning om en person i ett ärende om fingerade uppgifter på begäran av Polismyndigheten. Polismyndigheten har ansvar att bistå en person med fingerade personuppgifter vid kontakter med andra myndigheter samt i övrigt lämna den hjälp som krävs, om den enskildes hjälpbehov inte kan tillgodoses på annat sätt. Medgivandet upphör om den enskilde själv skriftligen anmäler hos Polismyndigheten att det inte längre behövs. Om det finns särskilda skäl kan även Polismyndigheten besluta att medgivandet ska upphöra.

Fingerade personuppgifter har inget skydd i de systemstöd som används i en region eller kommun eftersom de hanteras som vilken person som helst.

3.4. Offentlighets- och sekretesslagen reglerar utlämning av allmänna handlingar

Offentlighets- och sekretesslagen (OSL) ersatte sekretesslagen 2009 i syfte att göra den mer lättförståelig och lättillämpad. Lagen innehåller bestämmelser för hur myndigheter ska registrera, lämna ut och hantera allmänna handlingar. Det finns också regler om tystnadsplikt och förbud att lämna ut allmänna handlingar. En patients hälsotillstånd eller personliga förhållanden är exempel på vad som skyddas av sekretess.

Utöver de tre skyddsformerna (sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter) finns en särskild generell sekretessbestämmelse som gäller vissa personuppgifter om det av särskild anledning kan antas att den enskilde eller någon närstående till denne kan komma att utsättas för hot eller våld eller lida annat allvarligt men om uppgiften röjs (21 kap. 3 § första stycket OSL).

Sekretessen gäller uppgift om en enskilds

- bostadsadress eller annan jämförbar uppgift som kan lämna upplysning om var den enskilde stadigvarande eller tillfälligt bor
- telefonnummer
- e-postadress eller annan jämförbar uppgift som kan användas för att komma i kontakt med personen.

Sekretessen gäller även för motsvarande uppgifter om personens anhöriga. Bestämmelsen gäller oavsett sammanhang som uppgiften förekommer i.

3.5. Patientdatalagen ökar patientsäkerheten med bibehållet skydd för den personliga integriteten

Patientdatalagens syfte är att öka patientsäkerheten med bibehållet skydd för den personliga integriteten. Här finns bestämmelser om hur vårdgivare ska behandla personuppgifter inom hälso- och sjukvården och hur patientjournal ska föras. Lagen kompletteras av föreskrifter och allmänna råd samt handbok från Socialstyrelsen.

Patientdatalagen och Socialstyrelsens författning om journalföring och behandling av personuppgifter i hälso- och sjukvården ställer krav på unik identifiering av både patienter och personal i vårdgivarnas informationssystem som innehåller patientuppgifter. Vårdgivare behöver därför rutiner för hur skyddade personuppgifter ska hanteras.

Dokumentation av olika åtgärder i journalen kan vara avgörande för patientsäkerheten. Dokumentationen är även viktig som underlag för rättsintyg för att bedöma om ett brott har begåtts eller inte.

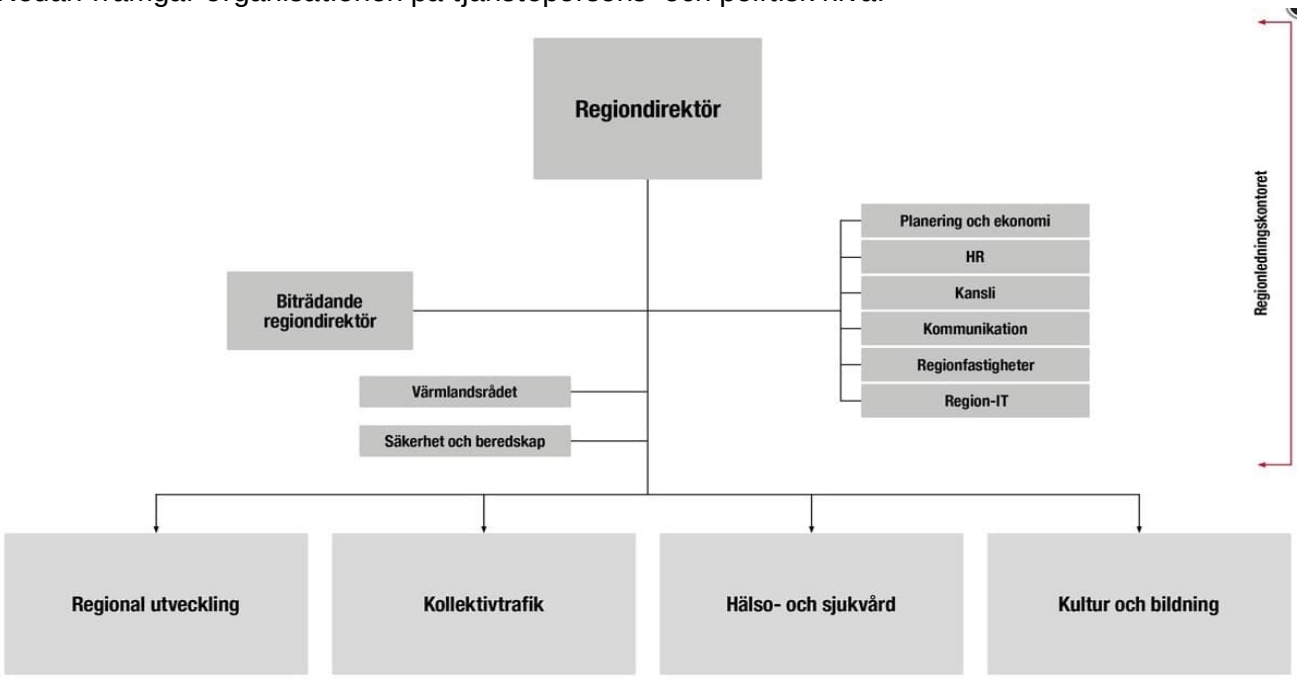
4. Organisation och ansvar

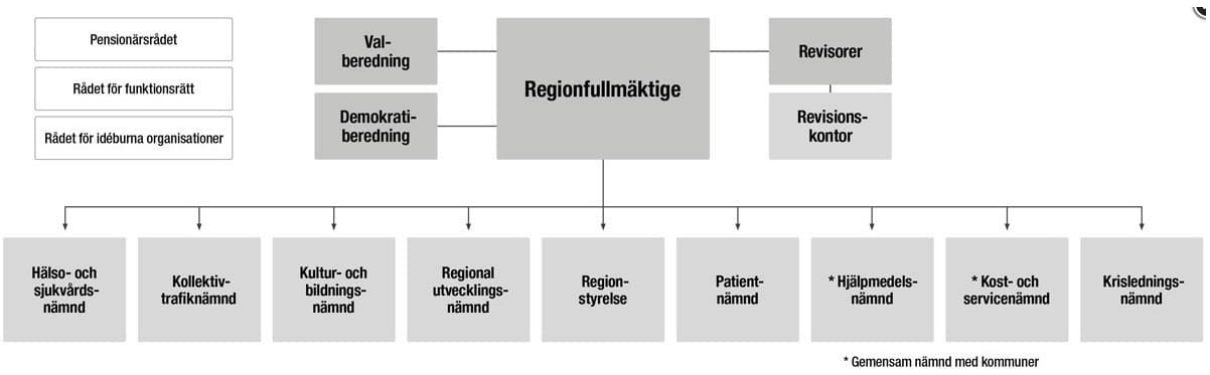
4.1. Personuppgiftsansvaret är delat mellan styrelse och nämnder

Regionstyrelsen är regionens ledande politiska organ. Styrelsen ska leda Region Värmlands verksamhet genom att utöva samordning och leda arbetet med att ta fram förslag på styrdokument till regionfullmäktige. Styrelsen ska vidare ha ett övergripande ansvar för interna säkerhetsfrågor och ansvara för strategiska frågor om informationssäkerhet.

Regionstyrelsen är anställningsmyndighet för all personal men varje nämnd ansvarar för personal inom sitt verksamhetsområde. Respektive styrelse/nämnd är personuppgifts-ansvarig för register och behandlingar av personuppgifter som sker i styrelsens/ nämndens verksamhet.

Nedan framgår organisationen på tjänstepersons- och politisk nivå.





5. Styrning och uppföljning

5.1. Det finns en rad olika riktlinjer med tillhörande rutiner vid hantering av skyddade personuppgifter

Inom regionens verksamheter finns en rad regionövergripande och verksamhetsspecifika riktlinjer, rutiner och anvisningar vad gäller hanteringen av skyddade personuppgifter. Dessa sammanfattas i tabellen nedan.

Ansvarig styrelse/nämnd[2]	Riktlinje/rutin/anvisning	Kort beskrivning
Regionstyrelsen	*”Skyddade personuppgifter”* (RIKT-22948-v.1.0)	Riktlinjen beskriver begreppet och hur regionen ska hantera personer med skyddade personuppgifter.
Regionstyrelsen	*”Skyddade personuppgifter avseende medarbetare”* (RIKT-24170-v.1.0)	Riktlinjen beskriver hur medarbetare med skyddade personuppgifter ska hanteras.
Regionstyrelsen	*”Avvikelsehantering”* (RIKT-18965-v.2.0)	Riktlinjen anger att medarbetare har lagstadgad skyldighet att rapportera observerade avvikelser och verksamhetschef/ motsvarande ansvarar för avvikelsehantering inom sitt område.
Regionstyrelsen	*”Rapportering av informationssäkerhetsincidenter”* (RUT-18032-v.1.0)	Rutinen beskriver arbetsprocessen vid inrapportering av informationssäkerhetsincidenter.
Regionstyrelsen	*”Rapportera informationssäkerhetsincidenter”* (INS-21315-v.2.0)	Instruktionen uppmärksammar att listor med känsliga personuppgifter innebär en risk för informationssäkerhetsincidenter. Instruktionen beskriver hur rapportering av incidenter ska ske i avvikelsehanteringssystemet ”AHA”.
Hälso- och sjukvårdsnämnden	*”Skyddade personuppgifter i Hälso- och sjukvård samt tandvård”* (RIKT-23133-v.1.0)	Riktlinjen beskriver hur hälso- och sjukvården ska hantera patienter med skyddade personuppgifter.
Hälso- och sjukvårdsnämnden	*”Patienter med skyddade personuppgifter i Cosmic”* (RUT-06670-v.12.0)	Rutinen gäller för hela hälso- och sjukvårdsverksamheten och beskriver hur patienter med skyddade personuppgifter ska hanteras i vårdinformationssystemet Cambio Cosmic.
Hälso- och sjukvårdsnämnden	*”Patienter med skyddade personuppgifter i Carita”* (RUT-23412-v.1.0)	Rutinen gäller Folktandvården och beskriver hur skyddade personuppgifter ska behandlas i vårdinformationssystemet Carita.
Hälso- och sjukvårdsnämnden	*”Skyddade personuppgifter – arbetssätt”* (INS-12519-v.3.0)	Instruktionen gäller för psykiatrisk öppenvård - psykiatrisk mottagning Kristinehamn och beskriver mottagningens arbetssätt för patienter med skyddade personuppgifter.
Hälso- och sjukvårdsnämnden	*”Hantera patienter med skyddade personuppgifter”* (INS-22808-v.4.0)	Instruktionen gäller för bild- och funktionsdiagnostik och fungerar som komplement till övergripande riktlinjer och rutiner.
Hälso- och sjukvårdsnämnden	*”Hantering av skyddade personuppgifter”* (INS-22945-v.1.0)	Instruktionen gäller för vårdcentralsområde västra Värmland Jourcentralen Säffle, VC Säffle Nysäter.

[2] Riktlinjerna är inte antagna av regionstyrelse och/eller nämnder.

		Den ska säkerställa att all personal känner till och följer regionens riktlinjer samt lokala rutiner.
Kollektivtrafiknämnden	*”Skyddade personuppgifter - kollektivtrafik”* (diarienummer framgår ej)	Rutinen specificerar arbetsprocess för de tre enheterna inom kollektivtrafiken som hanterar personer med skyddade personuppgifter.
Kultur- och bildningsnämnden (folkhögskolornas styrelse)	*”Riktlinjer för skyddande av personuppgifter gällande studerande på regionens folkhögskolor”* (ej fastställd)[3]	I rutinen klarläggs vad som innefattas av skyddsvärda personuppgifter och hur arbete ska ske med dessa.
Patientnämnden	*”Skyddade personuppgifter”* (RUT-23577-v.1.0)	Rutinen täcker hur personer med skyddade personuppgifter ska hanteras inom patientnämndsenheten.
Regionala utvecklingsnämnden	-	Regionala utvecklingsnämnden saknar egna styrdokument och använder de regionövergripande riktlinjerna.

Regionfullmäktige har 2019-10-17 fastställt ”Styrande dokument - struktur, fastställande och hantering” som anger att en riktlinje ger förutsättningar och styrning för hur något ska genomföras det vill säga anger ramarna för handlingsutrymmet inom ett visst område eller ämne. En riktlinje får fastställas av regionfullmäktige, regionstyrelse eller nämnd. I undantagsfall kan regiondirektör, direktör eller verksamhetschef (eller av utsedd befattningshavare) fastställa en riktlinje om den gäller ren verkställighet.

5.2. Flertalet internkontrollplaner omfattar inte risker vid hantering av skyddade personuppgifter

Regionstyrelsens, Hälso- och sjukvårdsnämndens, Kollektivtrafiknämndens, Regionala utvecklingsnämndens eller Patientnämndens internkontrollplaner omfattar inte risker vid hantering av skyddade personuppgifter.

I Kultur- och bildningsnämndens internkontrollplan för 2022 finns en identifierad risk med bäring på hantering skyddade personuppgifter. Risken är formulerad: *”Verksamhetens informationstillgångar ges inte ett tillräckligt skydd.”* Vidare har folkhögskolornas styrelse identifierat en risk med direkt bäring på skyddade personuppgifter i internkontrollplanen för 2022. Risken lyder: *”Skyddande av personuppgifter”.* Åtgärder för att minska risken är att regionens riktlinjer ska göras kända på folkhögskolorna samt att berörd personal ges utbildning vilket ska följas upp årligen samt rapporteras till nämnd i tertialrapport 2.

5.3. IT och informationssäkerheten är centraliserad

Regionstyrelsen har övergripande ansvar för interna säkerhetsfrågor och ansvarar för strategiska frågor om informationssäkerhet. Ändamålsenliga systemstöd är en väsentlig del av ett framgångsrikt arbete för att garantera säker hantering av patienter, elever och medarbetare med skyddade personuppgifter.

[3] Riktlinjen är inte slutligt fastställd men är tänkt att spegla folkhögskolornas arbete. Den är enligt intervjuade förankrad hos informationssäkerhetssamordnare som också är kontaktperson för regionens hantering av skyddade personuppgifter.

Driften av nationella IT-system som hanterar kontroll av personuppgifter mot befolkningsregistret och 1177 hanteras av Inera AB som ägs av regioner, kommuner och SKR.

Företaget tillhandahåller e-hälsotjänster inklusive vårdinformationstjänsten 1177 Vårdguiden. I övrigt hanteras driften av de stora vårdinformationssystemen av extern part via så kallade molntjänster eller av regionen själva.

Regionen använder förvaltningsstyrningsmodellen Pm3[4] för förvaltning av IT-baserade system. IT-verksamheten är centraliserad inom regionen, förvaltningen och underhåll av IT-system sköts i samverkan mellan IT centralt med respektive verksamhet. Enligt IT-chef och dataskyddssamordnare pågår processer för att samordna och prioritera nyutveckling och underhåll mellan verksamheterna i syfte att skapa samordningsvinster och stordriftsfördelar. I samband med detta kommer Pm3-modellen att fasas ut till förmån för central portföljsstyrning som följer övrig linjeorganisation. Det poängteras att den lokala kompetensen i verksamheten är viktig.

Det finns inget ledningssystem för informationssäkerhet och i intervjuer framkommer uppfattningen att det saknas en helhetsbild samtidigt som det uppges finnas god kontroll över vilka svagheter som finns i regionens IT- och informationssäkerhet. Regionen klassar information på verksamhetsnivå för informationssäkerhetsbedömning och det uppges vara ett verksamhetsansvar att bedöma informationens känslighet. En utmaning beskrivs vara att bedöma vad som är det *mest kärnfulla* i informationssäkerhetsarbetet. Det krävs därför ökad medvetenhet om betydelsen av informationssäkerhet i hela organisationen, inte endast inom hälso- och sjukvården där sekretessfrågor är vanligt förekommande. Det lyfts fram att personuppgifter förekommer i många verksamhetssystem och att försiktighet och hög riskmedvetenhet måste upprätthållas.

Penetrationstester som identifierar vilka sårbarheterna är och hur stor skada de kan orsaka, genomförs oregelbundenhet men det planeras för ökad regelbundenhet. Penetrationstest i syfte att kontrollera hanteringen av skyddade personuppgifter har inte genomförts eller planerats.

5.4. Kansliavdelningen ansvarar för övergripande administration

Inom Regionstyrelsens ansvarsområde finns kansliavdelningen som svarar för övergripande administration. Intervjuer har genomförts med kanslidirektör, enhetschef för rättsenheten och enhetschef för sekretariatet. De beskriver svårigheter med att nå ut med riktlinjer, rutiner och anvisningar till nyanställda och det finns behov att arbeta mer organiserat med utbildning. Den stora regionala organisationen beskrivs vara en utmaning där varje enskild verksamhet har fokus på sitt ansvarsområde.

Det finns en central informationssäkerhetssamordnare som är kontaktperson åt hela regionen vad gäller skyddade personuppgifter, och särskilt med informationssäkerhet för hälso- och sjukvård samt folktandvård. Av intervju framgår önskemål att samordnaren ska arbeta mer regionövergripande så dennes kompetens kan spridas bättre.

I samband med intervju identifierades risk avseende hanteringen av avvikelser.

[4] Pm3 är en modell som beskriver hur systemförvaltning ska organiseras för att kunna bedrivas på ett affärsmässigt sätt. Pm3 har förvaltningsobjektet som utgångspunkt och tydliggör förvaltningsverksamheten och dem gemensamma affärer som denna utgör för verksamhetsparter och IT-parter.

Det sägs finnas ett mörkertal då det inte går att garantera att samtliga avvikelser verkligen inrapporteras. Rapporteringen bygger på att enskilda individer gör som anvisat och i stressade situationer kan misstag ske. Det finns därmed risk för att nuvarande uppgifter, alltså inga avvikelser alls avseende skyddade personuppgifter, inte stämmer med verkligheten.

Det upplevs behövas bättre analyser av risk för avvikelser, och avvikelser, samt hur de aggregeras, systematiseras och överförs till övergripande nivå där samband kan iakttas, ett lärande ske som kan återföras till organisationen för att stärka rutinerna ytterligare.

Av intervjuer framkommer även risk för konflikt mellan olika prioriteringar, exempelvis hälso- och sjukvårdens prioritering av säker hälso- och sjukvård för enskild patient framför perspektivet att inte röja någons personuppgift.

Vidare beskrivs att risken för röjning ökar ju fler personer med åtkomst till IT-system kopplade till varandra, vilket är fallet idag.

5.5. Regionservice ansvarar för receptionerna och telefonväxeln i hälso- och sjukvården

Regionservice är en serviceorganisation som finns för regionens verksamheter, patienter, besökare, medarbetare, externa vårdgivare, kommuner och övriga intressenter. Regionservice ansvarar bland annat för servicetjänster inom lokalvård, logistik, kost samt kundservice. Reception och telefonväxel hanterar dagligen personer som ringer med frågor kring specifika patienter. Det finns rutiner och systemstöd för vad receptionisterna får och inte får säga. Vid inkommande samtal från myndighet, exempelvis polisen, ska medarbetare motringa till myndighetens telefonväxel. Det uppges finnas en upparbetad vana kring hantering av patientsekretess. Vid hotfulla situationer påkallas ordningsvakt/väktare.

5.6. Det förekommer medarbetare med skyddade personuppgifter

I regionen fanns vid granskningstillfället anställda med skyddade personuppgifter och som framkom ovan finns en nyligen upprättad riktlinje för hanteringen av medarbetare med sådant skydd. HR-direktör påtalar att varje medarbetare har stort eget ansvar att upplysa om förekomsten av skyddade personuppgifter antingen vid anställningstillfället, under anställningsintervju eller då sådant skydd uppstår under anställningen. I riktlinjen saknas dock information om *vilka* funktioner som ska, eller bör, informeras. Det beskrivs vara något den enskilda medarbetaren och dennes närmaste chef får överenskomma om.

Kunskapsnivån beskrivs vara otillräcklig. Farhågan är att inte alla verksamheter har vetskap om hur frågan ska hanteras. Då det finns riktlinje för hanteringen av medarbetare i regionen beskrivs det finnas goda förutsättningar att fokusera på kunskapsspridning och skapa större medvetenhet i hela organisationen. I nästa delkapitel följer mer specifika iakttagelser för varje verksamhetsområde kopplat till hanteringen av medarbetare med skyddade personuppgifter.

5.7. Respektive verksamhetsområde står inför unika utmaningar

5.7.1 Hälso- och sjukvårdsnämnden

Inom hälso- och sjukvårdens ansvarsområde beskrivs det finnas stor kompetens och vana att hantera känsliga personuppgifter, däribland skyddade. Behandling av patienter med skyddade personuppgifter är en sällanföreteelse men förekommer.

Det ingår således i yrkeskunskapen att hantera patienters personuppgifter genom journalföring och remisshantering. Hälso- och sjukvårdens rutiner kring hanteringen av patienter med skyddade personuppgifter beskrivs därför vara ändamålsenliga och välkända bland medarbetarna.

Samtidigt beskrivs det som en utmaning att nå ut med riktlinjer, rutiner och anvisningar till samtliga medarbetare som träffar patienter trots att hälso- och sjukvården har omfattande informationsspridningsprocesser, exempelvis genom att riktlinjer och rutiner tas upp på arbetsplatsträffar.

Målet är att skapa *vaksamhet* bland samtliga medarbetare då det inte kan förväntas att varje medarbetare kan ha förkunskap om exakt hur varje uppkommen situation ska hanteras. Informationssäkerhetssamordnare beskriver att det finns risk om det skapas instruktioner som avviker från befintliga rutiner eftersom säkerhet främjas av upprepning, inte av alternativa handlingssätt.

Vad gäller anställda med skyddade personuppgifter anses det inte lika långt kommet att skapa tydlig och trygg hantering. Det beskrivs som en gråzon i hur medarbetare med skyddade personuppgifter ska hanteras. Praktiska frågor som hantering av namnbricka, porträttfoton på väggar och journalföring lyfts fram. Det beskrivs även vara en utmaning att upprätta heltäckande riktlinjer, rutiner och anvisningar då varje situation anses kräva unik hantering. I nuläget hanteras uppstådda situationer via samtal mellan berörd medarbetare och chef om hur medarbetaren önskar få sina uppgifter hanterade. En grundläggande princip är att så få personer som möjligt ska ha vetskap om den specifika medarbetarens skyddade personuppgifter. Det tolkas som att informationen ska stanna mellan aktuell medarbetare, närmaste chef och eventuella ytterligare medarbetare utifrån den skyddade medarbetarens önskemål.

I samband med intervju identifierades risk avseende när barn med skyddade personuppgifter då en av föräldrarna utgör det hot barnet ska skyddas ifrån. Denne förälder kan fortfarande vara vårdnadshavare och besitta rätt att ta del av uppgifter som rör barnet. Båda vårdnadshavarna har laglig rätt att få kallelser till bokförd hemadress. Enligt intervjuade finns en ”lucka i lagen” som hälso- och sjukvården inte har möjlighet att undvika. Det är en sällanföreteelse men måste hanteras från fall till fall och orsakar osäkerhet.

I undantagsfall har hälso- och sjukvården valt att föra journal på papper enligt vad rutinen för *Skyddade personuppgifter i Hälso- och sjukvård samt tandvård* anger. Det är i situationer då den som utgör hotet har anställning i regionen, eller kontakter inom regionen, med tillgång till journaler. Det ska ha inträffat vid två tillfällen och journaler på papper ska användas mycket restriktivt, enbart i undantagsfall eftersom de medför andra former av risker. Det ska ske i samråd med regionjurist.

Vidare beskrivs att telefonkontakter med privatpersoner är särskilt känsliga och innebär ökad risk för röjning av skyddade personuppgifter. Det händer inte helt sällan att någon ringer och frågar efter patient eller medarbetare. Det finns upprättade rutiner för hur sådana situationer ska hanteras som anger att personuppgifter aldrig ska utlämnas om det inte på förhand har kommunicerats med patienten. Krypterad e-post finns inte men ska enligt uppgift införas hösten 2022.

Folktandvården uppger att de under längre tid påtalat behovet av automatiska loggkontroller.

Idag görs regelbundet manuella loggkontroller men det kräver särskild uppmärksam att notera om anställd läst journalen för en patient med skyddade personuppgifter. Enligt uppgift ska automatiska loggkontroller införas i Folktandvården i likhet med de som redan finns inom övrig hälso- och sjukvård.

Vad gäller avvikelsehantering rapporteras och hanteras alla avvikelser inom regionen i det gemensamma avvikelsehanteringssystemet ”AHA”. Det åligger chefer på alla nivåer att analysera, sammanställa och följa upp avvikelser inom respektive ansvarsområde. Det beskrivs finnas god kännedom om hur informationssäkerhetsavvikelser ska undvikas och hanteras. Det går dock inte att särskilja avvikelser för skyddade personuppgifter gentemot andra informationssäkerhetskategorier utan att göra manuell sökning.

Det beskrivs som ett medvetet val och inte vara ett problem då särbehandling av skyddade personuppgifter inte är eftersträvansvärt. Det framhålls att olika typer av avvikelser hanteras dagligen och att eventuella röjningar av skyddade personuppgifter inte anses mer allvarligt än någon annan avvikelse. Särbehandling anses kunna skapa förvirring med risk för felhantering. Statistik från rapporterade avvikelser hanteras per enhet men aggregeras och överförs inte till övergripande nivå för hälso- och sjukvårdens verksamhet. Ingen avvikelse kring skyddade personuppgifter uppges ha inträffat sedan regionen bildades 1 januari 2019.

Inom Folktandvården finns sedan 2017 fyra rapporterade avvikelser vad gäller skyddade personuppgifter. Avvikelsehanteringssystemet (AHA) anses emellertid inte anpassat till att registrera sådana avvikelser då det saknas specifik kategori för just den formen av avvikelser. Det görs inga sammanställningar över anmälda avvikelser och särredovisning av denna typ av avvikelser uppfattas därför som mindre intressant/inte nödvändigt.

5.7.2 Kollektivtrafiknämnden

Kollektivtrafiken är allmän där alla ska kunna resa och därför finns inte information och kunskap om kollektivtrafikens enskilda resenärer. En vuxen resenär som reser med vuxenkort behöver ingen legitimation. I de fall resan sker med skolkort eller annat rabatterat kort kan resenären dock bli avkrävd legitimation. Om någon uppgift då inte stämmer görs en sökning i bokföringsregistret ”Infotorg”. Personer med skyddade uppgifter saknar dock adressuppgift i Infotorg och Intervjuade påtalar att stort ansvar åligger individen. Resenären med skyddade personuppgifter måste vara extra försiktig och exempelvis avstå från att resa med rabatterad biljett.

Innevarande rutin för kollektivtrafiken är så nyligen fastställd att det beskrivs svårt att avgöra om den har fått tillräckligt genomslag i organisationen. Under intervjun nämns ordet ”nyvaken” i samband med hanteringen av skyddade personer. Nämnden har inte genomfört någon risk- och konsekvensanalys för risk för röjning av skyddade personuppgifter.

Fakturor skickas per post via Skatteverket förmedlingstjänst till de med skyddade personuppgifter. Personuppgifter per e-post undviks i den mån det är möjligt och hanteras i övriga fall med försiktighet. Hantering beskrivs dock alltid vara ett riskmoment. Enligt intervjuade pågår ett arbete att upprätta en e-tjänstportal som möjliggör inloggning med Bank-ID.

Enligt intervjuade finns i dagsläget inte anställda med skyddade personuppgifter. Om det skulle bli aktuellt kontaktas HR-avdelningen för rådgivning.

Eventuella avvikelser kan rapporteras på flera sätt. Som tidigare beskrivits går det i dagsläget inte att kategorisera eventuella avvikelser som avser specifikt skyddade personuppgifter. Vid personuppgiftsärenden finns som rutin att vända sig direkt till regionens dataskyddsombud.

5.7.3 Kultur- och bildningsnämnden

Riskmomentet kring röjning av skyddade personuppgifter finns i kultur- och utbildningsnämndens samt folkhögskolornas interkontrollplaner för 2022 och föranleddes av att den regionövergripande riktlinjen fastställdes hösten 2021.

I regionens folkhögskolor förekommer elever med skyddade personuppgifter.

Skolorna beskrivs därför vara vana att hantera sådant och verksamhetssystemet SchoolSoft är anpassat till att hantera skyddade personuppgifter. Alla skolor uppges således ha samma förutsättningar att hantera på ett korrekt sätt enligt gällande rutiner.

Det finns inga rutinbeskrivningar kring skoladministratörernas tillvägagångsätt vid hantering av elever med skyddade personuppgifter. Tillämpat arbetssätt bygger på de enskilda administratörernas erfarenhet och bedömning.

Sökande till utbildning som har skyddade personuppgifter hänvisas till skoladministratör. Det finns möjlighet att ansöka med hjälp av pappersblankett som förvaras i kassaskåp som endast skoladministratören har tillgång till. En ansökningshandling förvaras i två år innan den makuleras. Det är sökande själv som ansvarar för att beskriva vilka uppgifter som ska markeras som skyddade i systemet. Exempelvis finns möjligheten att ange fiktivt namn men vid sidan av e-postadress och kontaktuppgift till nära anhörig finns inga övriga krav på personlig information. Skoladministratören verifierar lämnade uppgifter genom kontroll med folkbokföringsregistret, Navet.

Utöver två skoladministratörer känner klassföreståndare till att det finns elev med skyddade personuppgifter, men endast om eleven själv väljer att berätta. Det skiljer sig mycket mellan elever hur öppna de väljer att vara. Vissa vill att mycket information ska framgå på Schoolsoft och berättar för lärare och studiekamrater medan andra inte vill informera alls. Det bygger på elevens medgivande som denne muntligt uppger vid ansökan samt vad eleven själv väljer att berätta till lärare och andra elever. Medgivandet dokumenteras inte. Efter intervjun framkom att skoladministratör tagit fram utkast till medgivandeblankett som ska vara obligatorisk för sökande eleven att skriva på vid ansökningstillfället eller senare vid behov av revidering. Syftet är att synliggöra allvaret i att information delas med andra samt att trygga personalens situation kring vad som får delas.

Hög medvetenhet och noggrannhet bland samtlig personal framställs som avgörande för en säker hantering. Medvetenhet beskrivs som god bland rektorer, lärare och administrativ personal. Utbildningen och kunskapsspridning kan emellertid stärkas då det finns viss personalomsättning. Verksamheterna använder den övergripande riktlinjen för skyddade personuppgifter, dock har folkhögskolorna tagit fram förslag på kompletterande rutin som inte är antagen än.

Framgångsfaktorn för säker hantering beskrivs vara utbildning och kunskapsspridning av gällande rutiner i hela organisationen. Kunskapen om regionens övergripande och verksamhetsspecifika rutiner förmedlas framför allt av Hälso- och sjukvårdsnämndens informationssäkerhetssamordnare.

Det beskrivs dock fortsatt finnas behov av ytterligare kunskapsspridning och utbildningsinsatser framför allt för Kultur- och bildningsnämndens specifika verksamhetsområden. Många anställda har exempelvis inte utbildats i ämnet. En utmaning beskrivs vara att regionens organisation är uppdelad i ”stuprör” där tvärsektionellt arbete och informationsutbyte inte sker i tillräcklig utsträckning. Samverkan mellan förvaltningarna vad gäller informationssäkerhet i allmänhet, och skyddade personuppgifter i synnerhet, beskrivs behöva förbättras.

Vidare beskrivs att ytterligare utbildningsinsatser för bland annat nyanställda och gästföreläsare är nödvändigt.

I samband med intervju identifierades risk avseende verksamhet som bedrivs i stiftelseform såsom Wermlands Opera och Värmlands Museum. Intervjuade beskriver den delade ansvarsfördelningen mellan regionen och Karlstad kommun som en gråzon till följd av delade huvudmannaskap som resulterar i att det saknas utpekat uppföljningsansvar exempelvis för hantering av skyddade personuppgifter.

I samband med intervju identifierades andra riskmoment, däribland vikarierande lärare eller gästföreläsare som inte är insatta i regionens rutiner och som kommer i kontakt med elever med skyddade personuppgifter. Detsamma gäller studiekamrater som inte har vetskap om att vissa uppgifter är känsliga och inte får röjas.

För medarbetare med skyddade personuppgifter beskriver intervjuade att det finns anställda bland regionens folkhögskolor med sådant skydd och att kontakt i första hand etableras med HR- avdelningen vid rekrytering av exempelvis lärare med skyddade personuppgifter. Stödet som HR-avdelningen erbjuder är huvudsakligen välfungerande genom den nyligen framtagna rutinen för hantering av medarbetare med skyddade personuppgifter.

Eventuella avvikelser rapporteras i regionens avvikelsehanteringssystem AHA. Det finns inga avvikelser registrerade vad gäller skyddade personuppgifter men det anses otillförlitligt och går inte att likställa med att avvikelser inte inträffat, endast att inga uppmärksammats.

5.7.4 Regionala utvecklingsnämnden

Regionala utvecklingsnämnden har ingen verksamhetsspecifik rutin och använder de regionövergripande riktlinjerna. Det hanteras väldigt få personuppgifter inom verksamheten eftersom det sällan förekommer kontakt med enskilda personer. Däremot är kontakter med organisationer och företag vanliga även om personuppgifter är ovanliga även i dessa fall. Vad gäller företagsstöd är alla personuppgifter sekretessklassade.

Det finns inga rapporterade avvikelser kopplat till hanteringen av skyddade personuppgifter. Incidenter anses aldrig ha aldrig ägt rum och erfarenhet om hanteringen är därmed begränsad. Intervjuade hänvisar till den regionövergripande riktlinjen men poängterar att vetskapen om riktlinjen och kunskapen om hanteringen av skyddade personuppgifter i verksamheten behöver stärkas då de sällan eller aldrig kommer i kontakt med personuppgifter. Det beskrivs vara svårt att hålla en rutin levande när förekomsten är sällsynt.

Vad gäller eventuella medarbetare med skyddade personuppgifter saknas kännedom. Om det skulle förekomma tas kontakt med HR-avdelningen.

Det saknas kunskaper om vilka risker knutna till personuppgifter som finns i organisationen och var dessa är som störst. Det uppges finnas behov av att genomföra risk- och konsekvensanalys i syfte att säkra rutinerna.

5.7.5 Patientnämnden

En person som fått vård har möjlighet att lämna klagomål till Patientnämnden. Patientnämndsenheten hanterar ca 1 600 ärenden per år. Klagomål kan lämnas via 1177 via inloggning med mobilt Bank-ID, via telefon eller brev. Ett klagomål kan dock inte rapporteras via e-post då den inte är krypterad.

Om klagomål anmäls via telefon finns möjlighet att vara anonym men då utan möjlighet till återkoppling på lämnat klagomål.

Patientnämndsenheten analyserar inkomna ärenden och sammanställer informationen men utan att använda personuppgifter. Klagomålen rör allt som har med hälso- och sjukvård samt tandvård att göra, alltifrån bristande journalhantering och bemötande av vårdpersonal till eventuella brister i hanteringen av skyddade personuppgifter.

Det samlade resultatet av klagomål redovisas i samband med nämndmöten samt i delårsrapport och årsredovisningen till Patientnämnden.

Vidare har Patientnämndens presidium och Hälso- och sjukvårdsnämndens arbetsutskott årliga dialog- och informationsmöten där material ur analyser kan diskuteras och det som bedöms relevant lyftas till Regionstyrelsen.

Patienten kan, förutom att själv lämna klagomål, låta anhörig med fullmakt göra det. På regionens externa hemsida finns information om hur du lämnar klagomål på vården. Det finns dock ingen specifik information om hur klagomål som rör hanteringen av skyddade personuppgifter kan lämnas.

I de fall patient vill lämna klagomål har denne ett egenansvar att uppge förekomst av skyddade personuppgifter. Vill patienten ha svar finns möjlighet att skicka svaret till Skatteverket eller till annan adress patienten uppgett.

Alla underlag sparas i dokumentskåp. Nämndens rutin för hanteringen av skyddade personuppgifter beskrivs vara ändamålsenlig och känd bland samtliga kollegor. Även om det sällan kommer in denna typ av ärenden ska samtliga medarbetare vara väl insatta i gällande rutiner. Vad gäller regionen i sin helhet beskrivs det finnas en generell risk för röjning ju fler personer som hanterar skyddade personuppgifter och att det kräver en extra ”fyrkantig” behandling av just dessa personuppgifter för att undvika risk för röjning.

Det finns inga anmälda ärenden vad gäller hanteringen av skyddade personuppgifter men det går inte i systemet att särskilja ärenden som avser skyddade personuppgifter, dessa måste spåras manuellt. Orsaken är inte känd och det är osäkert om det betyder att det inte finns några händelser eller om informationen om möjligheten att anmäla sådana ärenden via Patientnämnden inte är tillräckligt tydlig.

Vad gäller medarbetare med skyddade personuppgifter beskrivs att ett stort ansvar åligger den enskilde att själv avgöra vilken information som ska delges chef och övriga medarbetare.

5.8. Bedömning

Nämnderna har gemensamma men även specifika utmaningar. Enligt reglementet har Regionstyrelsen ett övergripande ansvar för interna säkerhetsfrågor och ansvar för strategiska frågor om informationssäkerhet. Regionstyrelsen är anställningsmyndighet för all personal men varje nämnd ska samtidigt ansvara för personal inom sitt verksamhetsområde. Respektive styrelse/nämnd är personuppgiftsansvarig för de register och andra behandlingar av personuppgifter som sker i styrelsens/nämndens verksamhet. Ansvaret är således delat och vi bedömer att risk föreligger att det försvårar samordning och ansvarstagande för hantering av personer med skyddade personuppgifter.

Samtliga granskade interkontrollplaner, med undantag för Kultur- och bildningsnämnden, saknar risk- och konsekvensanalyser över skyddade personuppgifter. I intervjuer påtalas att kunskap om riskerna och deras hantering ska skötas verksamhets- och professionsnära och är inget de förtroendevalda kan engagera sig i eftersom regionens verksamheter och ansvar är så omfattade och komplexa. Det är emellertid en relativt enkel metod, och ansvar, att tillse att interna kontroller finns och tillämpas samt vilka resultat dessa ger. Att så inte sker (med undantag för Kultur- och bildningsnämnden) är därför en brist.

Vi bedömer att upprättade riktlinjer, rutiner och anvisningar i huvudsak är utförliga och behandlar nödvändiga beskrivningar av hanteringen av personer med skyddade personuppgifter men det finns behov av utförligare regionövergripande och verksamhetsspecifika beskrivningar som är baserade på risk- och konsekvensanalyser.

Riktlinjer, rutiner och anvisningar är nyligen framtagna vilket kräver tid för implementering i hela organisationen vilket regionen bör vara uppmärksam på.

Styrdokumentens inbördes ordning är av betydelse, de principiella (exempelvis policys), antas av Regionfullmäktige, regionövergripande (exempelvis riktlinjer) av Regionstyrelse och nämnder medan rutinbeskrivande dokument lämpar sig för förvaltningens beslut. Av granskningen framkommer att samtliga styrande dokument avseende skyddade personuppgifter är antagna på chefsnivå vilket härstammar från en riktlinje som regiondirektör antog, daterad 2021-01-07 och rubricerad ”Skyddade personuppgifter Gäller för: Region Värmland”. Den anger att alla riktlinjer för övriga verksamhet ska antas av respektive direktör. Mot bakgrund av att regionfullmäktige beslutat att riktlinjer endast i undantagsfall får antas av chefer bedömer vi att en översyn bör ske av dokumentens klassificering samt vilka som ska antas av regionstyrelsen, facknämnder respektive av chefsfunktioner.

Det finns risker inom respektive verksamhetsområden som inte inkluderats i antagna riktlinjer, rutiner och anvisningar. Vissa styrande dokument är utformade på ett otydligt sätt i situationer där anställda efterfrågar konkreta regler och metodanvisningar. Det finns risker av allmän karaktär som gäller hela regionen, exempelvis kommunikation med myndigheter, ändamålsenliga systemstöd, telefonkontakt med privatpersoner, avvikelsehanteringen, brister i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare och tydligare rutiner för hanteringen av medarbetare. Vidare finns det mer verksamhetsspecifika risker.

Kompetens och kunskapsspridning är ett särskilt utvecklingsområde. Medvetandegrad och kunskapsnivån behöver stärkas genom exempelvis obligatoriska utbildningar och ökad informationsspridning.

Informationssäkerhetssamordnaren arbetar särskilt med informationssäkerhet för hälso- och sjukvården och Folktandvården samt fungerar som kontaktperson för skyddade personuppgifter i hela regionen. Det saknas dock en spridd kunskap om informationssäkerhetssamordnares roll som kontaktperson och det bör övervägas om denne kan axla ett tydligare ansvar som compliancefunktion det vill säga ett samordnande ansvar för att styrande dokumenten är relevanta, kända och tillämpade.

Hälso- och sjukvården hänvisar till den kompetens som verksamheterna har kring sekretess och att detta stärker hanteringen av skyddade personuppgifter.

Generellt delar vi den bedömningen men framhåller att då anställda och vårdtagare med skyddade personuppgifter är relativt sällan förekommande inom de flesta verksamheter kan detta leda till ökad risk för felaktig hantering. Hög personalomsättning innebär också en ökad risk.

Då risken att röja skyddade personuppgifter inte bedömts och värderats utifrån risk- och konsekvensanalyser är bedömningen att Regionstyrelsen och granskade nämnder inte genomfört relevanta kontrollåtgärder.

6. Stickprovskontrollen visar att det finns vissa brister i hantering av personer med skyddade personuppgifter

I granskningen har det genomförts stickprov av den faktiska följsamheten till regelverket och kontrollerat att systemstöd är ändamålsenliga för hantering av skyddade personuppgifter. De granskade systemen är:

- Vårdinformationssystem, Cambio Cosmic som sammanhållen journalföring
- Avvikelsehantering (AHA)
- Loggrapporter
- Elevregister
- Lönelistor och HR-system

6.1. Vårdinformationssystem

Kontrollen visar att person med skyddad folkbokföring framgår genom att patientlistan i Cosmic är markerad med tydlig textrad ”Skyddade personuppgifter”. Fälten i patientkortet för adressuppgifter är tomt och möjligheten att dokumentera kontaktuppgifter i patientkortet är frånkopplat. Personnummer framgår. Det går inte att använda fiktiva namn i Cosmic.

6.2. Avvikelsehantering

I avvikelsehanteringssystemet AHA har det inhämtats sammanställning för åren 2019 till 2021 över informationssäkerhetsavvikelser och GDPR samt sammanställningen av avvikelser kopplat till informationssäkerhet, GDPR och personuppgiftsincidenter som regionstyrelse och respektive nämnd får del av.

Antal avvikelser de tre senaste åren är 88. Utöver det finns 120 avvikelser som avser allt från försenade remisser till felkopplade samtal i växel. Inga avvikelser avser skyddade personuppgifter.

Sammanställningen av avvikelser finns i den årliga informationssäkerhetsrapporten som styrelse och respektive nämnd får del av.

I den rapporterar informationssäkerhetssamordnaren vilka granskningar och skyddsåtgärder av större betydelse som gjorts, informerar om riskanalyser och händelseanalyser som genomförts samt vilka förbättringsåtgärder som utförts. Informationssäkerhetsrapporten för 2020 och 2021 var vid granskningstillfället inte färdigställd varför rapporten för 2019 granskats. Av den framkommer att personuppgiftsincidenter ägt rum - dock ingen avseende skyddade personuppgifter.

6.3. Loggrapporter

Ansvaret för regelbunden och systematisk granskning av logghändelser sker i vårdinformationssystemet och åligger verksamhetschefer. Händelser ska regelbundet loggas. På förekommen anledning kan loggutdrag göras för uppföljning eller på begäran av patient exempelvis vid misstanke om röjning av skyddade personuppgifter. En logghändelse sparas i fem år. Logganalyser resulterar i rapporter. Vid misstanke om dataintrång sker utredning som kan resultera i avsked och polisanmälan. Gällande rutiner för loggkontroller omnämner inte skyddade personuppgifter. Hälso- och sjukvården genomför systematiska loggrapporter av den sammanhållna journalföringen.

Granskningen visar dock att detta inte genomförs i samtliga systemstöd, exempelvis i Schoolsoft samt Heroma.

6.4. Elevregister

Stickprovskontrollen i Schoolsoft omfattar elever med skyddade personuppgifter och det konstateras att systemet anger att eleven har skyddade personuppgifter samt visar de uppgifter eleven själv valt ska visas. Då det inte finns något skriftligt medgivande att dessa uppgifter får synas kan vi inte verifiera att det är rätt uppgifter som syns. All hantering i Schoolsoft loggas. Det framkommer dock inte vilka kontroller som görs av dessa loggar.

6.5. Lönelistor

Stickprovskontroll har utförts av HR-avdelningens hantering av skyddade personuppgifter i systemstödet Heroma.

Vi har bland annat tagit del av analyslista (kallad rapport) som kan tas ut av medarbetare på HR-avdelningen, löneenheten samt av ekonomer med behörighet. I rapporten står angivet med markerad text ”Rapporten innehåller personer med skyddad identitet” som följs med texten ”Innehållet i rapporten bör hanteras varsamt och inte spridas vidare då den inkluderar personer med skyddad identitet”. I analyslistan är personen som har skyddade personuppgifter markerad med texten ”Anonym” under personnumret.

Adressuppgifter förekommer inte men personens riktiga namn och personnummer förekommer. Det finns möjlighet för den enskilda personen att själv byta namnet till ett fiktivt men kräver manuell hantering. Vidare finns möjlighet att ange ett fiktivt namn vid anställningstillfället, men liksom hanteringen av elever som beskrivits ovan, undertecknas inte någon medgivandeblankett.

I samband med intervju identifierades risk avseende att det går att identifiera var i Region Värmland en anställd arbetar genom en enkel sökning i epostsystemet Microsoft Outlook, såvida den anställde inte använder fiktivt namn.

All hantering i Heroma loggas. Loggarna kontrolleras och analyseras dock inte automatiskt, utan på initiativ av HR-avdelningen.

6.6. Bedömning

De systemstöd som granskats i stickprovskontrollen är huvudsakligen ändamålsenliga för hantering av skyddade personuppgifter. I vårdinformationssystemet Cambio Cosmic, det skoladministrativa Schoolsoft och det personal- och löneadministrativa systemet Heroma framgår tydligt att personuppgifterna är skyddade.

Det finns dock brister i hanteringen av skyddade personuppgifter då det inte krävs skriftligt medgivande över vilka uppgifter som får användas, att Microsoft Outlook kan avslöja var i regionen en medarbetare arbetar samt att det inte görs systematiska eller automatiserade loggkontroller i samtliga system (däribland Schoolsoft och Heroma). I alla system som innehåller vårdinformation görs systematiska och regelbundna loggkontroller. Det är dock en brist att det i övriga verksamhetssystem inte görs loggkontroller kontinuerligt. Det finns behov av att informera personalen ytterligare, ta fram rutiner för loggarna genom att bestämma urval och omfattning av loggposterna, dokumentera logguppföljningen och följa upp bestämda rutiner samt införa automatiserade loggkontroller. Loggkontroller är ett effektivt verktyg att säkerställa att obehöriga inte får tillgång till skyddade personuppgifter.

Slutligen brister regionen i avvikelsehanteringen. Det är väsentligt att vårdgivare har god intern kontroll över den egna verksamheten med system för att identifiera, rapportera, åtgärda och följa upp avvikelser och risker. Vi noterar att det inte har rapporterats några avvikelser vad gäller skyddade personuppgifter, utöver inom Folktandvården. Orsaken till avsaknad av avvikelser kan bero på att möjligheten att registrera sådana ärenden via Patientnämnden eller i avvikelsehanteringssystemet AHA inte är tillräckligt känd. Flera intervjuade påtalar bristen att det inte går att kategorisera eventuella avvikelser som avser skyddade personuppgifter utan manuell hantering. Vi ser behov av kvalitetssäkrande åtgärder för att säkerställa att avvikelsehanteringssystemet återger en verklig bild. Därtill bedöms det att avvikelser behöver systematiseras och aggregeras i syfte att få en övergripande bild och skapa en lärprocess kring förbättringsåtgärder.

7. Samlad bedömning

7.1. Svar på revisionsfrågorna

Fråga	Svar
Har styrelse och nämnder tillsett att det finns ändamålsenliga rutiner för hantering av skyddade personuppgifter?	Nej. Dokumentgranskningen visar att det finns riktlinjer, rutiner och anvisningar men inga styrande dokument antagna av regionstyrelse eller nämnder. Befintliga riktlinjer är antagna av chefsfunktioner vilket härstammar från en övergripande riktlinje antagen av regiondirektör som gäller samtliga verksamheter och är styrande för verksamhetsamhetsspecifika riktlinjerna Därutöver finns en nyligen fastställd riktlinje för hanteringen av medarbetare med skyddade personuppgifter antagen av HR-direktör. Att förtroendevalda inte ges möjlighet att besluta om riktlinjer för skyddade personuppgifter bedöms stå i strid med fullmäktiges klassificering av styrdokument.

	Vi bedömer att riktlinjer, rutiner och anvisningar i huvudsak är utförliga och behandlar nödvändiga beskrivningar av hanteringen av personer med skyddade personuppgifter men att det finns behov av utförligare regionövergripande och verksamhetsspecifika beskrivningar baserat på risk- och konsekvensanalyser med stöd av eventuella avvikelser. Vissa styrande dokument är utformade på ett otydligt sätt i situationer där anställda efterfrågar konkreta regler och metodanvisningar. Riktlinjer, rutiner och anvisningar är nyligen framtagna och kräver tid för implementering i hela organisationen något som regionen bör vara uppmärksam på.
Har styrelse och nämnder säkerställt att det finns tillräcklig kunskap och erforderlig utbildning om gällande regelverk hos den personal som hanterar skyddade personuppgifter inom Region Värmland?	Nej. Kompetens och kunskapsspridning är ett särskilt utvecklingsområde. Inom respektive område, vid sidan av hälso- och sjukvården, finns behov av ökad medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter. Det saknas en lärprocess uppbyggd av erfarenheter och riskbedömningar inom och mellan respektive verksamhetsområde.
Har styrelse och nämnder tillsett att det sker en tillräcklig uppföljning och kontroll av att rutinerna efterlevs?	Nej. Risken att röja skyddade personuppgifter inte bedömts och värderats utifrån risk- och konsekvensanalyser. Därmed har Regionstyrelsen och granskade nämnder inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontroller att rutinerna efterlevs i regionen. Avvikelsehanteringen är inte kvalitetssäkrad och kan innehålla felaktig information då rutinerna kring inrapporteringen av avvikelser kopplade till skyddade personuppgifter inte anses säkerställda. Identifieringen av rapporterade avvikelser måste dessutom ske manuellt de skyddade personuppgifter inte har specifik kodning i systemet.
Har styrelse och nämnder säkerställt att obehöriga inte kan få tillgång till skyddade personuppgifter genom t. ex. användande av behörigheter och kontroller i olika datasystem?	Delvis. De systemstöd som granskats i stickprovskontroll är huvudsakligen ändamålsenliga för hantering av skyddade personuppgifter. Det finns dock brister i hanteringen av skyddade personuppgifter. - Det krävs inte skriftligt medgivande över vilka uppgifter som får användas. Det riskerar missförstånd och ett otydligt ansvar för uppgifterna eftersom den enskilde ytterst bär ansvar för vilka uppgifter som ska hanteras medan berörd nämnd ansvarar för hanteringen som sådan. - Microsoft Outlook kan röja var i regionen en medarbetare arbetar. - Det inte görs systematiska eller automatiserade loggkontroller i samtliga system. I alla system med vårdinformation görs systematiska och regelbundna loggkontroller.

	- Så sker inte i övriga verksamhetssystem. Det bör tas fram rutiner genom att bestämma urval och omfattning av loggposterna, dokumentera logguppföljningen, följa upp bestämda rutiner samt införa automatiserade loggkontroller. - Det är en brist att det inte genomförs penetrationstester av IT-systemen som kan identifiera sårbarheter och skadekonsekvenser.

7.2. Slutsatser och rekommendationer

Bedömningen är att Regionstyrelsen, Hälso- och sjukvårdsnämnden, Kollektivtrafiknämnden, Kultur- och bildningsnämnden, Regionala utvecklingsnämnden samt Patientnämnden inte i tillräcklig omfattning säkerställt intern styrning och kontroll.

Det finns ett antal riktlinjer, rutiner och anvisningar för hanteringen av personer med skyddade personuppgifter, inklusive medarbetare. Dessa styrande dokument bedöms i huvudsak vara utförliga och omfattar nödvändiga beskrivningar av hanteringen av personer med skyddade personuppgifter. Det finns dock behov av utförligare regionövergripande och verksamhetsspecifika beskrivningar baserat på inventerade riskmoment. Vissa styrande dokument är utformade på ett sätt som inte motsvarar det stöd som personal efterfrågar.

De riktlinjer som tillämpas bör enligt vår mening vara fastställda av regionstyrelse och berörda nämnder, inte som idag av chefsfunktioner, eftersom det kan stå i strid med regionfullmäktiges beslut om att riktlinjer endast i undantagsfall kan antas av chefer.

Det finns risker av allmän karaktär som gäller hela regionen, exempelvis extern kommunikation med myndigheter, ändamålsenliga systemstöd, telefonkontakt med privatpersoner, avvikelsehanteringen, brister i informationsspridning av riktlinjer, rutiner och anvisningar till medarbetare samt tydligare rutiner för hanteringen av medarbetare. Vidare finns verksamhetsspecifika risker som är unika för varje situation.

Vi uppmärksammar kompetens och kunskapsspridning som särskilda utvecklingsområden. Medvetandegrad och kunskapsnivå kring hanteringen av skyddade personuppgifter bör stärkas genom obligatoriska utbildningar och informationsspridning då mänskliga faktorn identifierats som stor risk i hanteringen av skyddade personuppgifter.

Risken för röjning av skyddade personuppgifter har inte bedömts och värderats utifrån genomförd risk- och konsekvensanalys. Regionstyrelsen eller granskade nämnder har därmed inte genomfört relevanta kontrollåtgärder. Styrelse och nämnder följer inte upp och kontrollerar att rutinerna efterlevs. Avvikelser systematiseras och aggregeras inte för att åtgärda brister kopplat till hanteringen av skyddade personuppgifter.

Utifrån granskningens iakttagelser rekommenderar vi Regionstyrelsen och granskade nämnder, utifrån sina respektive uppdrag och ansvarsområden, att tillse att det:

- Genomförs risk- och konsekvensanalyser avseende hantering av skyddade personuppgifter och vid behov lyfta in bedömda risker i internkontrollplanerna.
- Genomförs en översyn av de styrande dokumentens klassificering och beslutshierarki avseende skyddade personuppgifter i syfte att säkerställa så regionstyrelse och nämnder fastställer riktlinjerna.

- Genomförs obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument avseende skyddade personuppgifter samt avvikelsehantering, erfarenhetsanalys och i praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.
- Övervägs att inrätta ”compliancefunktion/-er”, det vill säga en funktion som ansvarar för att bestämmelser och interna verksamhetsprinciper, som exempelvis riktlinjer, rutiner och anvisningar, följs och följs upp. Detta för att hanteringen av skyddade personuppgifter ska vara prioriterat i regionens verksamheter.
- Genomförs penetrationstester av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång.
- Genomförs systematiska loggkontroller i samtliga systemstöd i syfte att säkerställa att obehöriga inte kan få tillgång till skyddade personuppgifter.
- Sker uppföljning av incidenter och avvikelser samt att avvikelsehanteringen avseende skyddade personuppgifter stärks.
-

Stockholm och Göteborg den 15 juni 2022

Jan Darrell
Certifierad kommunal yrkesrevisor, EY

David Leinsköld
Verksamhetsrevisor, EY

Magnus Andersson
Specialist och s*enior konsult inom IT-risk och informationssäkerhet, EY*

Mikaela Bengtsson
Kvalitetssäkrare
Certifierad kommunal yrkesrevisor, EY

Bilaga 1 Källförteckning

Intervjuade funktioner

- Kanslidirektör
- HR-direktör
- Regional utvecklingsdirektör
- Folkhälso- och kulturdirektör
- Hälso- och sjukvårdsdirektör
- Bitr. trafikdirektör
- IT-chef
- Dataskyddsombud
- Områdeschef Regionservice
- Driftchef Regionservice
- Enhetschef Regionservice
- Enhetschef rättsenheten Kansliavdelningen
- Enhetschef sekretariatet Kansliavdelningen
- Regionjurist
- Enhetschef patientnämndsenheten
- Informationssäkerhetssamordnare Hälso- och sjukvård
- Ledningsstrateg Regional utveckling
- Områdeschef Folkbildning
- Skoladministratör Kristinehamns folkhögskola
- Medicinskt ledningsansvarig Hälso- och sjukvård
- Områdeschef Slutenvård Hälso- och sjukvård
- Områdeschef Öppenvård Hälso- och sjukvård
- Områdeschef Vårdkvalitet Hälso- och sjukvård
- Tf. områdeschef Samverkan Hälso- och sjukvård
- Tandvårdschef Folktandvården
- Förvaltningsledare Folktandvården
- Systemförvaltare HR-avdelningen
- Avstämningskonsult HR-avdelningen
- Ordförande Regionstyrelsen
- Ordförande Hälso- och sjukvårdsnämnden
- Ordförande Kollektivtrafiknämnden
- Ordförande Regionala utvecklingsnämnden
- Ordförande Kultur- och bildningsnämnden
- Ordförande Patientnämnden

Granskad dokumentation

- Riktlinje för styrande dokument – struktur, fastställande och hantering, fastställd av regionfullmäktige 2019-10-17.
- Skyddade personuppgifter, fastställd av regiondirektör 2021-07-01.
- Skyddade personuppgifter avseende medarbetare, fastställd av HR-direktör 2022-04-11.
- Registrering och hantering av allmänna handlingar, fastställd av regiondirektör 2021-10-20.
- Avvikelsehantering, fastställd av regiondirektör 2020-09-01.
- Rapportering av informationssäkerhetsincidenter, fastställd av enhetschef kansliavdelningen 2020-08-21.
- Rapportera informationssäkerhetsincidenter, fastställd av enhetschef kansliavdelningen 2022-03-11.

- Registrering (diarieföring) av allmänna handlingar, fastställd av enhetschef sekretariatet.
- Personuppgiftsbehandling, fastställd av enhetschef kansliavdelningen 2020-08-21.
- Inhämtande av samtycke till behandling av personuppgifter, fastställd av enhetschef kansliavdelningen 2020-08-21.
- Skyddade personuppgifter i Hälso- och sjukvård samt tandvård, fastställd av hälso- och sjukvårdsdirektör 2021-10-06.
- Patienter med skyddade personuppgifter i Cosmic, fastställd av objektägare patientjournal 2021-10-13.
- Logghantering i Cosmic, fastställd av förvaltningsledare patientjournal 2020-02-02.
- Dataintrång – åtgärder vid misstanke om olovlig åtkomst, fastställd av objektägare patientjournal 2019-07-02.
- Logghantering vårdinformationssystem, fastställd av objektägare patientjournal 2021-05-03.
- Patienter med skyddade personuppgifter i Carita, fastställd av tandvårdschef 2022-01-20.
- Skyddade personuppgifter – arbetssätt, fastställd av enhetschef psykiatrisk öppenvård 2022-04-14.
- Hantera patienter med skyddade personuppgifter, fastställd av verksamhetschef bild- och funktionsdiagnostik 2022-03-10.
- Hantering av skyddade personuppgifter, fastställd av enhetschef Säffle vårdcentral 2021-08-02.
- Skyddade personuppgifter – kollektivtrafik, fastställd av informationssäkerhetssamordnare 2022-04-01.
- Utkast till Riktlinjer för skyddande av personuppgifter gällande studerande på regionens folkhögskolor.
- Skyddade personuppgifter, fastställd av enhetschef kansliavdelningen 2022-04-06.
- Informationssäkerhetsrapport 2019, RS/200590.