RIKS REVISIONEN

RiR 2024:6

Informationssäkerhet i vård och omsorg

– statens stöd och tillsyn

Riksrevisionen är en myndighet under riksdagen med uppgift att granska statliga myndigheter och verksamheter. Vi bedriver både årlig revision och effektivitetsrevision. Genom ett grundlagsskyddat oberoende har Riksrevisionen ett starkt mandat och är en viktig del av riksdagens kontrollmakt som bidrar till förbättringar och demokratisk insyn.

Denna rapport har tagits fram inom effektivitetsrevisionen, vars uppgift är att granska hur effektiv den statliga verksamheten är. Vi lämnar även rekommendationer för att förbättra den granskade verksamheten. Effektivitetsgranskningar lämnas direkt till riksdagen som bereder dem tillsammans med en svarsskrivelse från regeringen.

RIKS REVISIONEN

Riksrevisionen
RiR 2024:6
ISBN 978-91-7086-684-5
ISSN 1652-6597
Tryck: Riksdagstryckeriet, Stockholm 2024

RIKS REVISIONEN

Beslutad: 2024-03-26
Diarienummer: 2022/1031
RiR 2024:6

Till: Riksdagen

Härmed överlämnas enligt 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. följande granskningsrapport:

Informationssäkerhet i vård och omsorg

– statens stöd och tillsyn

Riksrevisionen har granskat om statens insatser för att stärka vård- och omsorgsgivares informationssäkerhetsarbete varit effektiva. Resultatet av granskningen redovisas i denna granskningsrapport. Den innehåller slutsatser och rekommendationer som avser regeringen, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten och Socialstyrelsen.

Riksrevisorn Helena Lindberg har beslutat i detta ärende. Revisionsledaren Nedim Colo har varit föredragande. Revisionsdirektören Olof Widmark och enhetschefen Magdalena Brasch har medverkat i den slutliga handläggningen.

Helena Lindberg Nedim Colo

För kännedom

Regeringskansliet; Försvarsdepartementet, Justitiedepartementet, Socialdepartementet

Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Myndigheten för samhällsskydd och beredskap, Socialstyrelsen

Innehåll

Sammanfattning

Vård- och omsorgsgivare hanterar stora mängder känsliga personuppgifter digitalt i många olika IT-system och ansvarar för informationssäkerheten för dessa personuppgifter. Det innebär bland annat att personuppgifter ska behandlas på ett sätt som säkerställer tillräckligt skydd. Staten ska stödja och kontrollera vård- och omsorgsgivares arbete med informationssäkerhet så att det sker systematiskt och riskbaserat enligt författningsreglerade krav. Flera statliga myndigheter har i uppdrag att styra, stödja, följa upp och bedriva tillsyn av vårdens och omsorgens informationssäkerhet. Riksrevisionens granskning visar att de statliga insatserna inte är effektiva. De åtgärder som regeringen och myndigheterna vidtagit har inte varit tillräckliga för att stärka vårdens och omsorgens informationssäkerhetsarbete och därmed höja deras informationssäkerhetsnivå. En central brist är att myndigheternas stöd inte är anpassat efter deras behov och att tillsynen är begränsad.

Stödet är inte tillräckligt anpassat efter vårdens och omsorgens behov

Integritetsskyddsmyndighetens (IMY:s), Myndigheten för samhällsskydd och beredskaps (MSB:s) och Socialstyrelsens stöd är inte effektivt för att stärka informationssäkerheten inom vården och omsorgen. Myndigheternas stöd är generellt och ger främst grundläggande vägledning när en verksamhet ska bygga upp ett systematiskt och riskbaserat informationssäkerhetsarbete. Men stödet är inte tillräckligt anpassat efter vård- och omsorgsgivares behov så att det kan omsättas i det praktiska informationssäkerhetsarbetet. Det handlar exempelvis om frågor som berör säkerhetsåtgärder i avvägningar mellan informationssäkerhet, integritet och patientsäkerhet vilket kräver stöd vid tolkning av lagstiftningen. Myndigheterna har i stor utsträckning valt att inte göra rättsliga ställningstaganden för hur kraven i bestämmelserna som gäller för vården och omsorgen kan tolkas, vilket försvårar för vård- och omsorgsgivare att förstå vad som förväntas av dem.

Det är framför allt mindre kommuner som har begränsade resurser och svårt att rekrytera personal med den kompetens som krävs för att systematiskt arbeta med och säkerställa tillräcklig informationssäkerhet. Bristande stöd från de statliga myndigheterna kan därför leda till varierande skyddsnivåer för personuppgifter i olika delar av landet. Varken MSB, IMY eller Socialstyrelsen anser sig ha ansvar att tillgodose vårdens och omsorgens behov av specifikt stöd. Myndigheterna arbetar också i stuprör och har inte samverkat eller samordnat sina insatser när de utformar sitt stöd. Granskningen visar dessutom att MSB:s och IMY:s stöd vid inträffade IT-incidenter är begränsat. Vård- och omsorgsgivare som drabbas av exempelvis cyberangrepp får sällan operativt stöd från MSB för att lindra effekterna av det inträffade.

Tillsynen är begränsad och det är oklart om den inriktas mot verksamheter där den gör mest nytta

Inspektionen för vård och omsorgs (IVO:s) och IMY:s tillsyn av vårdens och omsorgens informationssäkerhet bidrar inte till att stärka skyddet av personuppgifter på ett effektivt sätt. Sedan 2018, när dataskyddsförordningen och lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) trädde i kraft, har IMY och IVO genomfört få tillsynsärenden av vårdgivare och inga alls av omsorgsgivare. Dessutom har tillsynen sällan omfattat alla delar av en verksamhets informationssäkerhet. IVO har också bedrivit begränsad tillsyn enligt NIS-lagen, vilket innebär att myndigheten inte fullt ut har granskat den faktiska säkerheten i vårdgivarnas informationssystem och nätverk där personuppgifter hanteras. Sammantaget innebär detta att statens kontroll av vård- och omsorgsgivares informationssäkerhet och efterlevnad av förvaltningsenliga krav inte är effektiv. Det resulterar även i att de verksamheter som omfattas av tillsynen inte får tillräckligt med vägledning i hur de kan förbättra sitt informationssäkerhetsarbete. Dessutom är tillsynen bara delvis riskbaserad, vilket gör att det är svårt att bedöma om den fokuserar på verksamheter där den skulle ge störst nytta. IMY och IVO har inte följt upp tillsynsbesluten, och det är därför oklart om de granskade verksamheterna har åtgärdat de brister som identifierats vid tillsynen.

Regeringen har inte sett till att styrningen är sammanhållen

Regeringen har vidtagit få åtgärder för att stärka vårdens och omsorgens informationssäkerhetsarbete. Regeringen har inte tydligt fastställt ansvars- och uppgiftsfördelningen mellan IMY, MSB och Socialstyrelsen när det gäller att utforma stöd som motsvarar vårdens och omsorgens behov. Regeringen har inte heller sett till att myndigheterna samordnar sitt arbete för att effektivt utforma stödet. Trots att omsorgen ofta hanterar lika känsliga personuppgifter som vården, har regeringen inte verkat tillräckligt för att omsorgsgivare ska omfattas av samma tydliga krav på säkerhetsåtgärder och systematiskt informationssäkerhetsarbete som vårdgivare, förutom när det gäller viss behörighetstilldelning och kontroll av behörigheterna.

Rekommendationer

Till regeringen

- Förtydliga Socialstyrelsens ansvar för att ta fram verksamhetsanpassat stöd till vårdens och omsorgens informationssäkerhetsarbete. Stödet bör utformas utifrån vård- och omsorgsgivares behov och i samråd med relevanta myndigheter. Stödet kan bland annat innebära att:
    - identifiera sektorsspecifika risker och sårbarheter för informationssäkerhet.

    - ge exempel på lämpliga organisatoriska och tekniska säkerhetsåtgärder för informationssäkerhet.
    - ge stöd och vägledning i hur bestämmelserna för skydd av personuppgifter bör tolkas i generella fall.
- Utred hur omsorgsgivare fullt ut kan omfattas av motsvarande bestämmelser för skydd av personuppgifter som vårdgivare.
- Säkerställ att omsorgsgivare och mindre vårdgivare som inte omfattas av NIS-lagen omfattas av krav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Till Inspektionen för vård och omsorg

- Bedriv tillsyn som granskar om vårdgivare faktiskt uppfyller NIS-lagens samtliga krav på säkerhet i nätverk och informationssystem.
- Utveckla arbetet med riskanalyser så att tillsynen i större utsträckning inriktas mot områden där bristerna i informationssäkerhet är som störst.
- Utveckla uppföljningen av tillsynsbeslut för att säkerställa att tillsynen får avsedd effekt.

Till Integritetsskyddsmyndigheten

- Effektivisera handläggningen av klagomåls- och tillsynsärenden och frigör därigenom resurser för att bedriva mer riskbaserad tillsyn.
- Utveckla arbetet med riskanalyser så att tillsynen i större utsträckning inriktas mot områden där bristerna i informationssäkerhet är som störst.
- Utveckla uppföljningen av tillsynsbeslut för att säkerställa att tillsynen får avsedd effekt.

1 Inledning

1.1 Motiv till granskning

Regeringens mål är att Sverige ska bli bäst i världen på digitalisering av vård och omsorg till 2025.[1] Vården och omsorgen hanterar stora mängder känsliga personuppgifter digitalt i många olika IT-system. Digitaliseringen innebär en stor utvecklings- och effektiviseringspotential[2] men medför också nya och förändrade typer av hot och risker.[3] För att främja digitaliseringen är det enligt riksdagen och regeringen viktigt att skydda patientens integritet.[4]

Regioner och kommuner ansvarar för informationssäkerheten inom vården och omsorgen. Det innebär att de ska vidta säkerhetsåtgärder för att skydda personuppgifter när de används, lagras och delas digitalt. Om informationen är felaktig, går förlorad, är otillgänglig eller inte skyddas från obehöriga kan det få allvarliga konsekvenser för individer. Det kan även skada förtroendet för digitala tjänster och minska tilliten till vården och omsorgen. Dessutom kan bristande informationssäkerhet bli kostsamt[5] och utgöra en risk för patientsäkerheten om sjukvårdspersonal inte har tillgång till nödvändig patientinformation.[6]

Det finns brister i regionernas och framför allt kommunernas informationssäkerhetsarbete, som är på en generellt låg nivå.[7] Myndigheten för samhällsskydd och beredskap (MSB) har bland annat konstaterat att säkerhetsåtgärder ofta implementeras av kommunerna utan att de föregåtts av riskanalyser och utan att följas upp.[8]

Flera myndigheter har i uppdrag att bedriva tillsyn och ge stöd till regionernas och kommunernas informationssäkerhetsarbete. Ansvaret är delat mellan myndigheterna. Regionerna och framför allt kommunerna uppges ha svårt att i praktiken tillämpa MSB:s stöd för informationssäkerhetsarbete i den egna verksamheten. De uppges också ha svårt att tolka bestämmelserna i dataskyddsförordningen och relevant nationell lagstiftning. Det råder också brist på kompetens inom informationssäkerhet, särskilt bland kommunerna.[9] MSB bedömer att många kommuner inte avsätter tillräckligt med resurser för att höja nivån i informationssäkerhetsarbetet. MSB:s egen uppföljning visar att myndigheten bland annat behöver förbättra sitt råd och stöd och sina utbildningsinsatser.[10] Det är också

1 Regeringsbeslut S2020/00574/FS.
2 Prop. 2020/21:1 Utgiftsområde 9, s. 40.
3 SOU 2015:23, *Informations- och cybersäkerhet i Sverige*, s. 64.
4 Prop. 2007/08:126, bet 2007/08:SoU16, s. 10, rskr. 2007/08:207.
5 SVT, ”Miljonkostnader för Kalix kommun efter IT-attacken”, hämtad 2022-01-14.
6 SOU 2022:6, s. 455–456.
7 Framgår bland annat av MSB:s och Socialstyrelsens undersökningar. Se avsnitt 2.4.
8 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, 2022, s. 54 f.
9 Intervju med företrädare för SKR, 2022-09-07.
10 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, 2022, s. 19, 30–32.

oklart vilket operativt stöd som vård- och omsorgsgivare får när allvarligare IT-incidenter väl sker, såsom cyberangrepp.

De rättsliga bestämmelserna om informationssäkerhet för personuppgifter är omfattande och komplexa. Denna komplexitet, tillsammans med bristen på kompetens och resurser, ökar risken för att informationssäkerhetsarbetet inte bedrivs på ett systematiskt och enhetligt sätt och för att nivån på informationssäkerhet därmed avviker från vad som krävs utifrån skyddsbehovet inom vården och omsorgen.

Det är oklart hur Inspektionen för vård och omsorgs (IVO:s) och Integritetsskyddsmyndighetens (IMY:s) tillsyn har bedrivits. Statskontoret konstaterade 2020 att IMY hade avslutat få tillsynsärenden sedan 2015 och att tillsynen var delvis riskbaserad samt att handläggningstiderna är långa.[11]

Det förändrade säkerhetshetspolitiska läget och återkommande cyberangrepp mot regioner och kommuner har satt ytterligare fokus på riskerna med deras bristande informationssäkerhetsarbete. Riksrevisionen har mot bakgrund av detta granskat statens arbete för att stärka vårdens och omsorgens informationssäkerhet.

1.2 Övergripande revisionsfråga och avgränsningar

Den övergripande revisionsfrågan är: Är statens arbete för att stärka skyddet av personuppgifter som hanteras digitalt inom vård och omsorg effektivt? För att skydda personuppgifter ska en verksamhet bedriva ett informationssäkerhetsarbete. Den övergripande granskningsfrågan besvaras med följande delfrågor:

- Är myndigheternas arbete med att styra och stödja vårdens och omsorgens informationssäkerhetsarbete effektivt?
- Är myndigheternas tillsyn av vårdens och omsorgens informationssäkerhet effektiv?

Granskningen omfattar regeringen, MSB, Socialstyrelsen, IMY och IVO. Med myndigheternas styrning avses huvudsakligen förordningar och föreskrifter som de har ansvar för att ta fram. Med stöd avses bland annat råd, vägledningar, stödmaterial, stödfunktioner och utbildningar som myndigheterna ansvarar för. Informationssäkerhet täcker in all information som en organisation hanterar. Granskningen fokuserar på informationssäkerhet för personuppgifter, som regioner och kommuner ansvarar för och hanterar digitalt inom vården och omsorg.

Med vård avses ansvaret för sådana insatser som bedrivs inom ramen för hälso- och sjukvårdslagen (2017:30), HSL. Omsorg, som är en del av socialtjänsten, definieras i granskningen som ansvaret för insatser till äldre personer och personer med funktionsnedsättning. Med vårdgivare avses i granskningen den som bedriver vård

[11] Statskontoret, *Myndighetsanalys av Datainspektionen*, 2020, s. 31, 38.

enligt HSL.[12] Med omsorgsgivare avses den som utför insatser för äldre personer eller personer med funktionsnedsättning.[13] Vård- och omsorgsgivarna kan vara en statlig myndighet, region, kommun, annan juridisk person eller en enskild näringsidkare. Vi har i granskningen särskilt fokuserat på verksamhet som bedrivs i regional eller kommunal regi.

Granskningen omfattar inte länsstyrelsernas stöd till kommuner i deras kontinuitetsarbete.[14] Granskningen omfattar heller inte det grundläggande ansvar inför och under fredstida kriser och höjd beredskap som åvilar kommuner och regioner, till exempel vad gäller upprätthållandet av kritisk infrastruktur.[15] Vidare omfattar inte granskningen informationssäkerhet enligt säkerhetsskyddslagen (2018:585) eller Polismyndighetens insatser.[16]

1.3 Bedömningsgrunder

För att bedöma om de statliga insatserna för att stärka skyddet av personuppgifter inom vård och omsorg är effektiva utgår vi från bedömningsgrunder, som är de kriterier som vi tillämpar för att värdera våra iakttagelser.

En övergripande utgångspunkt för Riksrevisionens bedömning av de statliga insatserna är myndigheternas uppdrag att utfärda föreskrifter, ge stöd och bedriva tillsyn av vård- och omsorgsgivares informationssäkerhet för personuppgifter. Flera författningar ställer krav på informationssäkerhet hos såväl regionala och kommunala vård- och omsorgsgivare som enskilda.

De övergripande målen för hälso- och sjukvården och socialtjänsten är att vården och omsorgen ska vara jämlik och av god kvalitet.[17] För att uppnå dessa mål har riksdag och regering bland annat möjliggjort ökad digital delning av personuppgifter inom och mellan vård- och omsorgsgivare.[18] Vid införandet av patientdatalagen (2008:355) (PDL) ansåg riksdagen att det är mycket viktigt att skydda patientens integritet eftersom detta är avgörande för om patienten kommer att ge samtycke till att personuppgifter hanteras och delas i system med en digitalt sammanhållen journal.

---

12 Enligt 2 kap. 3 § hälso- och sjukvårdslagen (2017:30) är en vårdgivare en statlig myndighet, region, kommun, annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet.

13 Enligt 1 § lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation är en omsorgsgivare en myndighet i kommun eller region som har ansvar för eller utför insatser för äldre personer eller personer med funktionsnedsättning, samt andra juridiska personer eller enskilda näringsidkare som utför sådana insatser. I granskningen använder vi begreppet i en allmän mening för verksamheter som bedriver omsorg om äldre och personer med funktionsnedsättning inom ramen för Socialtjänstlagen.

14 4 § förordningen (2017:870) om länsstyrelsernas krisberedskap och uppgifter inför och vid höjd beredskap.

15 Se lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Jfr. aktuell översyn av bestämmelserna i Dir. 2023:51.

16 Det vill säga information som rör säkerhetsskyddsklassificerade uppgifter eller utgör en säkerhetskänslig verksamhet. Det skulle kunna handla om högspecialiserade vårdtjänster som efterfrågas i hela landet men som endast utförs av en vårdgivare.

17 3 kap. 1 § hälso- och sjukvårdslagen (2017:30) och 1 kap. 1 § och 3 kap. 3 § socialtjänstlagen (2001:453).

18 Prop. 2021/22:177, bet. 2021/22:SoU30, s. 20, rskr. 2021/22:381 och prop. 2007/08:126, bet 2007/08:SoU16, s. 18, rskr. 2007/08:207.

Enligt riksdagen måste skyddet av patientens integritet alltid komma i första rummet.[19] Regeringen har, med instämmande av riksdagen, i olika sammanhang betonat vikten av ett långsiktigt och metodiskt arbete som möjliggör för verksamhetens ledning att systematiskt styra informationssäkerheten.[20]

Granskningen utgår från att personuppgifter ska hanteras och skyddas så att obehöriga inte får tillgång till dem och att den personliga integriteten för de registrerade inte äventyras på annat sätt.[21] Flertalet uppgifter omfattas dessutom av bestämmelser om tystnadsplikt och sekretess.[22] Informationssäkerhet är en förutsättning för en säker hantering av personuppgifter, som bland annat framgår av artikel 32 i dataskyddsförordningen. Ett informationssäkerhetsarbete som är välavvägt och anpassat efter verksamhetens behov leder till ett kostnadseffektivt skydd och till att säkerhetsincidenter undviks.[23] För att åstadkomma detta behöver regioner och kommuner, enligt den nationella strategin för samhällets informations- och cybersäkerhet, bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.[24] Det innebär bland annat att de behöver utgå från kunskap om sårbarheter och införa de mest angelägna säkerhetsåtgärderna. Myndigheterna har i uppdrag att bedriva tillsyn och ge stöd till regioners och kommuners informationssäkerhetsarbete.

Enligt regeringen ska de statliga myndigheterna samordna sina stödjande insatser för systematiskt informationssäkerhetsarbete. För att åstadkomma detta utgår vi från att myndigheterna samverkar och utbyter kunskap i syfte att styra, stödja och utöva tillsyn av informationssäkerheten i vården och omsorgen på ett tydligt och samordnat sätt.[25] Krav på myndighetssamverkan uttrycks också i de rättsliga bestämmelserna som styr myndigheterna.[26]

Regeringens styrning och uppföljning av berörda myndigheters resultat och verksamhet är viktig i sammanhanget. Regeringen understryker att styrningen av statsförvaltningen ska vara långsiktig, strategisk, helhetsinriktad, sammanhållen, verksamhetsanpassad och tillitsbaserad. Detaljstyrning och onödig administration ska undvikas.[27] Vi utgår från att regeringen följer upp hur myndigheternas arbete med att

19 Prop. 2007/08:126, bet 2007/08:SoU16, s. 19, rskr. 2007/08:207.

20 Prop. 2017/18:205, s. 39 f., Skr. 2016/17:213, s. 8 och regeringsbeslut Ju2019/03058/SSK.

21 Se till exempel artikel 5.1 f dataskyddsförordningen som anger att den som behandlar personuppgifter säkerställa lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

22 25 kap. respektive 26 kap. offentlighets- och sekretesslagen (2009:400), OSL.

23 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, 2022, s. 22. Se även MSB, *Metodstöd för systematiskt Informationssäkerhetsarbete*, 2021, s. 6.

24 Skr. 2016/17:213 s. 8, bet. 2017/18:FöU4, s. 15, rskr 2017/18:142 och prop. 2017/18:205, s. 39.

25 Skr. 2016/17:213 s. 8-11, bet. 2017/18:FöU4, s. 8, rskr 2017/18:142.

26 Se samverkansskyldighet i 8 § förvaltningslagen (2017:900), 11 b § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap, 11 § förordningen (2015:284) med instruktion för Socialstyrelsen. Även tillsynsmyndigheterna omfattas av samverkan och kunskapsutbyte med de normerande och stödjande myndigheterna, se förordningen (2013:176) med instruktion för Inspektionen för vård och omsorg, Artikel 57 g dataskyddsförordningen. 21 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

27 Prop. 2020/21:1, utgiftsområde 2, s. 58, bet. 2020/21:FiU2, rskr. 2020/21:150.

stödja och bedriva tillsyn av vårdens och omsorgens informationssäkerhet fungerar och vidtar lämpliga åtgärder vid behov.

Utifrån MSB:s, IMY:s, IVO:s och Socialstyrelsens uppdrag har vi operationaliserat våra bedömningsgrunder för att kunna besvara den övergripande revisionsfrågan och delfrågorna. Om de angivna kriterierna inte är uppfyllda minskar sannolikheten för att statens samlade stöd och tillsyn ska fungera effektivt.

1.3.1 Operationaliserade bedömningsgrunder för delfråga 1

För att MSB:s, IMY:s och Socialstyrelsens styrning av och stöd till regioners och kommuners informationssäkerhetsarbete inom vården och omsorgen ska stärka deras förmåga att bedriva informationssäkerhetsarbete på ett effektivt sätt ska myndigheterna:

- ta fram föreskrifter som närmare preciserar aktuell lagstiftning[28]
- ha kompetens, effektiva processer och arbetssätt för att ta fram och utveckla stöd
- anpassa stödet efter vårdens och omsorgens olika behov, vilket bland annat innebär att stödet ska möjliggöra en säker hantering av personuppgifter enligt författningsreglerade krav
- se till att stödet är tydligt och lättillgängligt,[29] vilket bland annat innebär att stödet är samlat och uppdaterat
- samverka med varandra, och vid behov med andra aktörer, för att utbyta kunskap så att stödet är anpassat efter vårdens och omsorgens olika behov
- följa upp[30] och utvärdera[31] hur det egna stödet bidrar till att stärka deras informationssäkerhetsarbete, i syfte att kontinuerligt utveckla stödet.

1.3.2 Operationaliserade bedömningsgrunder för delfråga 2

IMY och IVO ska bedriva tillsyn för att säkerställa att vård- och omsorgsgivarnas informationssäkerhetsarbete bedrivs på ett sätt som skyddar personuppgifter i enlighet med kraven i lagstiftningen. För att tillsyn av vård- och omsorgsgivarnas informationssäkerhet ska vara effektiv ska myndigheterna:

- ha den kompetens, den organisation och de verktyg som krävs för att utföra den planerade tillsynen[32]

---

28 Se bilaga 1 för rättsliga bestämmelser för informationssäkerhet för personuppgifter.

29 Skr. 2016/17:213, s. 10, bet. 2017/18:FöU4, rskr 2017/18:142.

30 En uppföljning svarar på vad som har hänt och om det har gått enligt plan. Uppföljning kan fånga in resultat eller i ett tidigt skede indikera effekter i relation till ett uppsatt mål.

31 Utvärderingen bygger ofta på resultat från uppföljningen och syftar vanligen till att förstå och förklara prestationer och deras effekter.

32 Prop. 2012/13:20, s. 94 f., bet. 2012/13:SoU5, s. 9, rskr. 2012/13:116 och artikel 52.4 dataskyddsförordningen.

- planera och genomföra riskbaserad tillsyn med utgångspunkt i egna riskanalyser för att tillsynen ska ge störst nytta[33] (Analysen för inriktning av tillsynen bör omfatta en sammanvägd bedömning av var riskerna för väsentliga brister för informationssäkerhet är störst samt var bristerna riskerar att få störst konsekvenser.[34] En riskbaserad tillsyn förutsätter att myndigheten inhämtar tillräckligt med information om tillsynsobjekten och utarbetar bra processer och metoder för att göra riskanalyser.[35])
- handlägga tillsynsärenden effektivt och ha rimliga handläggningstider; enligt förvaltningslagen ska ett ärende handläggas så enkelt, snabbt och kostnadseffektivt som möjligt utan att rättssäkerheten eftersätts[36]
- följa upp tillsynsbesluten för att säkerställa att tillsynen fått avsedd effekt, vilket bland annat innebär att verksamheten har vidtagit åtgärder för att åtgärda brister i informationssäkerhetsarbetet
- ge råd och allmän vägledning vid tillämpningen av lagstiftningen inom ramen för sin tillsyn[37] och förmedla kunskap som erhålls genom tillsynen
- samverka med varandra så att tillsynen av informationssäkerhetsarbetet inom vård och omsorg ska bli samordnad.

1.4 Metod och genomförande

Vi har använt oss av intervjuer och dokumentstudier. Vi har genomfört 21 intervjuer med tjänstepersoner på IMY, IVO, MSB och Socialstyrelsen som arbetar med att utforma och ge stöd, och med företrädare för Sveriges Kommuner och Regioner (SKR).[38] Skriftliga frågor har besvarats av IMY, IVO, MSB och Socialstyrelsen samt Försvarsdepartementet, Justitiedepartementet och Socialdepartementet. Vi har tagit del av underlag från berörda myndigheter och avrapporteringar inom informationssäkerhetsområdet till regeringen.

För att granska i vilken utsträckning MSB:s, IMY:s och Socialstyrelsens stöd motsvarar regioners och kommuners olika behov av att stärka informationssäkerhetsarbetet inom vården och omsorg har vi genomfört intervjuer med företrädare för två regioner och sex kommuner i två län.[39] Vi har också granskat vilket stöd kommunerna fått från myndigheterna vad gäller hantering av pågående

33 1 och 2 §§ förordningen (2013:176) med instruktion för Inspektionen för vård och omsorg och IMY 2021, *IMY:s policy för tillsyn*. Se även Statskontoret 2020, *På väg mot en bättre tillsyn? En studie av den statliga tillsynens utveckling*.

34 Se även Statskontoret, *På väg mot en bättre tillsyn?*, 2020, s. 73–74.

35 Riksrevisionen, *Statens tillsyn över apotek och partihandel med läkemedel*, 2022, s. 31.

36 9 § förvaltningslagen (2017:900).

37 19 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster och artikel 57 b, c, v och artikel 58 3 a dataskyddsförordningen.

38 Kontaktpersonerna vid respektive myndighet har valt ut medarbetare och chefer som har deltagit vid intervjuerna.

39 Regionerna och kommunerna har anonymiserats i noterna i granskningsrapporten.

IT-incidenter, till exempel cyberangrepp. För detta ändamål har vi även intervjuat en kommun som varit utsatt för cyberangrepp.

Vi har tagit del av och analyserat dokumentation med relevans för de statliga myndigheternas uppdrag att ge stöd och utöva tillsyn av vård- och omsorgsgivares informationssäkerhet. Vi har närmare undersökt vilket stöd som finns tillgänglig, generellt och för vård- och omsorgsgivare, och hur stödinsatserna tagits fram och utformats av myndigheterna. Vi har också analyserat inkomna frågor som berör informationssäkerhet från regioner och kommuner och myndigheternas svar på dessa.[40] Undersökningen har kompletterats med intervjuer med företrädare för myndigheterna. Vi har också haft samtal med företrädare för SKR för att få en bild av deras stöd till kommuners och regioners informationssäkerhetsarbete. På motsvarande sätt har tillsynsmyndigheternas insatser undersökts. Vi har bland annat gått igenom och analyserat underlag till arbetet med riskanalyser, tillsynspolicyer, tillsynsplaner, statistik om genomförd tillsyn av vård- och omsorgsgivare 2018–2023, tillsynsbeslut, processbeskrivningar och handläggningstider.

Vi har valt att undersöka regioners och kommuners erfarenheter av det statliga stödet och tillsynen i de två största länen. I länen bor 40 procent av Sveriges befolkning, vilket innebär att regionerna och kommunerna i de två länen använder, lagrar och delar en stor del av personuppgifterna i Sverige. Vi har tagit hänsyn till kommunstorleken i regionen så att urvalet omfattar små-, medelstora- och stora kommuner. Intervjuerna inkluderade frågor om bland annat statens styrning, roll- och ansvarsfördelning, tillsyn av deras informationssäkerhetsarbete och stöd för informationssäkerhetsarbetet. Vi har också undersökt vilka behov av stöd som de har för att kunna stärka sitt informationssäkerhetsarbete.

Vi har även undersökt stödet från MSB vid en pågående IT-incident. Vi har därför intervjuat företrädare för en mindre kommun som utsattes för ett omfattande cyberangrepp under 2022. En mer utförlig beskrivning av urvalet finns i bilaga 2.

Granskningen har genomförts av en projektgrupp bestående av Nedim Colo (projektledare) och Olof Widmark. Henrik Segerpalm deltog i granskningen fram till juni 2023. Jurist Daniel Lindén Remstam, jurist Filippa Drakenmark och Arvid Åkerberg (praktikant) har också bidragit i arbetet. En referensperson har lämnat synpunkter på granskningsupplägg och på ett utkast till granskningsrapporten: Marika Ericson, jur.dr i folkrätt och biträdande prefekt vid Centrum för operativ juridik och folkrätt, Försvarshögskolan. Företrädare för Regeringskansliet (Försvarsdepartementet, Justitiedepartementet och Socialdepartementet), IMY, IVO, MSB och Socialstyrelsen har fått tillfälle att faktagranska och i övrigt lämna synpunkter på ett utkast till granskningsrapporten.

[40] Se bilaga 2 för mer utförlig beskrivning av vår genomgång av frågor och svar.

1.5 Disposition

Kapitel 2 är ett bakgrundskapitel som omfattar en beskrivning av informationssäkerhet samt de statliga myndigheternas uppdrag och uppgifter och regionernas och kommunernas brister i informationssäkerhetsarbete. I kapitel 3 redogör vi för statens arbete med att styra och stödja vård- och omsorgsgivarnas informationssäkerhetsarbete. I kapitel 4 redogör vi för myndigheternas tillsyn av vård- och omsorgsgivarnas informationssäkerhetsarbete. Kapitel 5 innehåller slutsatser och rekommendationer. Till rapporten hör också två bilagor.

2 Skyddet av personuppgifter inom vården och omsorgen

I detta bakgrundskapitel beskriver vi dels de bestämmelser som reglerar skyddet av personuppgifter i vården och omsorgen, dels det informationssäkerhetsarbete som syftar till att åstadkomma ett adekvat skydd för uppgifterna. Vi beskriver också de statliga myndigheternas uppdrag. Kapitlet avslutas med en sammanställning av de brister i regionernas och kommunernas informationssäkerhetsarbete som myndigheterna har identifierat.

2.1 Krav på skydd av personuppgifter

Flera olika bestämmelser reglerar skyddet av personuppgifter och ställer krav på regioner, kommuner och vård- och omsorgsgivare att bedriva ett informationssäkerhetsarbete som ska säkerställa skyddet av personuppgifter. Se bilaga 1 för mer utförlig beskrivning av bestämmelserna.

Skyddet av personuppgifter utgår från dataskyddsförordningen som trädde i kraft 2018. EU:s dataskyddsförordning är direkt tillämplig och har företräde framför nationell lagstiftning. Kärnan i förordningen är att skydda personers integritet och upprätthålla deras fri- och rättigheter.[41] Ett syfte är också att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU. Dataskyddsförordningen ställer krav på att personuppgiftsansvariga ska kunna visa att förordningen följs. En av principerna rör kravet på säkerhet[42] och innebär att personuppgifter ska behandlas på ett sätt som säkerställer lämpligt skydd, till exempel så att inte obehöriga får tillgång till personuppgifter och att de inte förloras eller förstörs. Skydd ska uppnås genom användning av tekniska eller organisatoriska[43] säkerhetsåtgärder som är lämpliga i förhållande till riskerna som behandlingen medför.[44]

I Sverige kompletteras dataskyddsförordningen av dataskyddslagen[45] och lagstiftning för olika områden vilka preciserar den övergripande lagstiftningen. När det exempelvis gäller individinriktad patientverksamhet som innefattar vård, undersökning eller behandling gäller PDL för personuppgiftsbehandlingen. I omsorgen preciseras den övergripande lagstiftningen dels av lagstiftning som gäller för hela socialtjänstens verksamhet, dels av lagstiftning som bara gäller omsorg. Både vården och omsorgen hanterar känsliga personuppgifter men regleringen för skyddet av personuppgifter är mindre preciserad i omsorgen.[46] (Se avsnitt 3.6.4.)

---

41 Artikel 1 och 2 dataskyddsförordningen. Dessförinnan gällde EU:s dataskyddsdirektiv (95/46/EG) med delvis motsvarande innehåll.

42 Mer preciserat ansvar för säkerheten i samband med behandling av personuppgifter regleras i artikel 32 i dataskyddsförordningen. Både den personuppgiftsansvarige och dennes anlitade biträden är skyldiga att följa denna artikel vilket innebär att båda dessa aktörer behöver vidta lämpliga säkerhetsåtgärder.

43 Till tekniska åtgärder räknas till exempel brandväggar, kryptering, pseudonymisering, säkerhetskopiering och anti-virus-skydd. Organisatoriska åtgärder handlar till exempel om interna rutiner och riktlinjer.

44 Se artikel 32 dataskyddsförordningen.

45 Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

46 Se Socialstyrelsen, *Säker personuppgiftsbehandling i socialtjänsten*, 2018.

Bestämmelser som reglerar skyddet av personuppgifter i vården och omsorgen

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). Lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Offentlighets- och sekretesslagen (2009:400), patientdatalagen (2008:355), patientdataförordningen (2008:360) och Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården. Lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, och förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten. Lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation.

Vårdgivares informationssäkerhet i nätverk och IT-system: Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen). Förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

MSB:s föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, MSB:s föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster, och MSB:s föreskrifter och allmänna råd (MSBFS 2018:9) om rapportering av incidenter för leverantörer av samhällsviktiga tjänster.

2.2 Ett systematiskt arbete med informationssäkerhet säkerställer att information skyddas

Kärnan i informationssäkerhet handlar om att styra och skydda information utifrån aspekterna konfidentialitet, riktighet och tillgänglighet så att rätt person har tillgång till rätt information vid rätt tillfälle.[47]

Informationssäkerhet innebär bevarande av *konfidentialitet* (endast behöriga får ta del av informationen), *riktighet* (att informationen inte är manipulerad) och *tillgänglighet* (att informationen finns när någon behörig efterfrågar den) hos information utifrån dess värde.[48]

Konfidentialitet är resultatet av en bedömning, ibland med stöd i lagar och andra krav.[49] Kraven på konfidentialitet grundar sig bland annat på bestämmelser om sekretess och dataskydd och till exempel PDL. Konfidentialiteten kan förändras över tid.

47 Ibland läggs även spårbarhet till som en aspekt.

48 3 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6) och MSB:s metodstöd för systematiskt informationssäkerhetsarbete, informationssäkerhet.se, ”Metodstöd”, hämtad 2024-02-06.

49 MSB, ”Termbanken för informationssäkerhet”, hämtad 2023-11-11.

Informationssäkerhet är en förutsättning för en säker hantering av personuppgifter. För att säkerställa skydd av personuppgifter i verksamheterna behöver regioner och kommuner bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.[50] Ett systematiskt informationssäkerhetsarbete är ett arbetssätt för att identifiera krav på och införa säkerhetsåtgärder som ger tillräckligt skydd för informationen utifrån ovan nämnda aspekter.[51] Säkerhetsåtgärder kan vara organisatoriska, personalrelaterade, fysiska eller tekniska. Det innebär att en verksamhet ska vidta de åtgärder som säkerställer att informationen skyddas, oavsett var den befinner sig och oavsett om den hanteras av människor eller i informationssystem. Verksamheten ska också kontinuerligt följa upp och utvärdera arbetet samt anpassa skyddet utifrån externa krav på organisationen, såsom lagstiftning, organisationens behov och risker. Centralt i arbetet är att klassa[52] informationen utifrån vad som kan hända om informationens konfidentialitet, riktighet och tillgänglighet inte upprätthålls.[53]

Kommuner och regioner omfattas inte av samma uttryckliga krav på att bedriva ett systematiskt informationssäkerhetsarbete som exempelvis statliga myndigheter.[54] Inom hälso- och sjukvården finns det däremot krav på vårdgivare att bedriva ett systematiskt informationssäkerhetsarbete i NIS-lagen.[55] NIS-lagen omfattar vårdgivare över en viss storlek.[56] Det saknas därmed uttryckliga rättsliga krav på mindre vårdgivare och omsorgsgivare att bedriva ett systematiskt informationssäkerhetsarbete.

2.3 De statliga myndigheternas uppdrag och ansvar

Flera statliga myndigheter har i uppdrag att styra, stödja, följa upp och bedriva tillsyn av vårdens och omsorgens informationssäkerhet. MSB har ett övergripande uppdrag att samordna arbetet med informationssäkerhet i samhället och ge stöd till verksamheter i alla sektorer. IMY ska ge vägledning till alla verksamheters arbete med att skydda personuppgifter.

Socialstyrelsen har som sektorsansvarig myndighet för hälso- och sjukvård och socialtjänst ett generellt ansvar för stöd och kunskapsutveckling inom sitt

---

50 Skr. 2016/17:213, s. 9–10, bet. 2017/18:FöU4, s. 15, rskr 2017/18:142.

51 Med systematiskt informationssäkerhetsarbete avses att arbeta strukturerat efter en bestämd process med analys, utformande och genomförande, samt uppföljning, utvärdering och förbättring. Att arbeta riskbaserat innebär att identifiera de risker som hänger samman med den information som verksamheten hanterar och anpassa skyddet av informationen utifrån denna analys.

52 Klassificering är en förutsättning för att skapa rätt skydd för informationen och undvika överskydd med onödigt höga kostnader och krångliga rutiner som följd.

53 MSB, *Metodstöd för systematiskt informationssäkerhetsarbete En översikt*, 2021.

54 De omfattas av inte av förordningen (2022:524) om statliga myndigheters beredskap och därmed inte av MSB:s föreskrifter (MSBFS 2020:6) om informationssäkerhet för statliga myndigheter.

55 Lagen syftar till att säkerställa en hög grad av säkerheten i bland annat hälso- och sjukvårdens nätverk och informationssystem.

56 7 kap. 1 § MSB:S föreskrifter (MSBFS 2021:9) om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. Leverantörer av samhällsviktiga tjänster inom hälso- och sjukvårdssektorn omfattas av lagen om antalet legitimerad vårdpersonal överstiger 50 årsarbetskrafter eller där minst 20 000 expedieringar av receptbelagda läkemedel utförs per år.

ansvarsområde. Tillsynen av informationssäkerhet i vården och omsorgen delas mellan IMY och IVO. IMY ska bedriva tillsyn av behandlingen av personuppgifter inom alla sektorer. IVO ska bedriva tillsyn av informationssäkerhet i vården och omsorgen utifrån gällande bestämmelser inom dessa områden. I följande avsnitt beskriver vi myndigheternas uppdrag närmare.

2.3.1 MSB ska normera och stödja informationssäkerhet inom alla sektorer

MSB har ansvar för frågor om skydd mot olyckor, krisberedskap och civilt försvar, i den utsträckning inte någon annan myndighet har ansvaret.[57] MSB ska stödja och samordna arbetet med samhällets informationssäkerhet. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till bland annat kommuner och regioner. MSB ska också bedöma omvärldsutvecklingen inom området.[58]

MSB har flera föreskriftsrätter som gäller informationssäkerhet. MSB ska meddela föreskrifter om bland annat vilka tjänster som är samhällsviktiga och om systematiskt och riskbaserat informationssäkerhetsarbete enligt NIS-lagen.[59] MSB ska även ge råd och stöd till IVO och Socialstyrelsen när de tar fram föreskrifter om säkerhetsåtgärder till NIS-lagen.[60] MSB ska också meddela föreskrifter om krisberedskap, vilka ställer krav på statliga myndigheters informationssäkerhetsarbete.[61]

MSB är enligt NIS-förordningen Sveriges nationella CSIRT-enhet (Computer Security Incident Response Team) för hantering av incidenter som rapporteras enligt NIS-lagen.[62] MSB ska ta emot incidentrapporter från leverantörer av samhällsviktiga tjänster och tillgängliggöra informationen för IVO och Socialstyrelsen.[63] MSB ansvarar också för Sveriges CERT-funktion (Computer Emergency Response Team) som har i uppgift att stödja samhället i arbetet med att förebygga och hantera IT-incidenter. MSB ska agera skyndsamt vid IT-incidenter genom att sprida information om incidenter och hot till bland annat regioner och kommuner i förebyggande syfte. När en verksamhet drabbas av IT-incidenter ska MSB vid behov arbeta med samordning av åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekterna av det inträffade. MSB ska återrapportera till berörda

57 1 § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap.

58 11a § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap.

59 4 och 17 §§ NIS-lagen och 3 och 7 §§ NIS-förordningen. MSB har utfärdat tre föreskrifter till NIS-lagen, (MSBFS 2021:9) föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster, (MSBFS 2018:8) föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster och (MSBFS 2018:9) föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster.

60 8 § NIS-förordningen.

61 26 § förordningen (2022:524) om statliga myndigheters beredskap. Den ersatte förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

62 2 § NIS-förordningen. Se även 11 och 12 §§ NIS-lagen.

63 18 § NIS-lagen och 12 § NIS-förordningen.

aktörer i samband med att en IT-incident har rapporterats och samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet.[64]

MSB ska rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället. MSB ska också årligen lämna en rapport till regeringen med en sammanställning av de IT-incidenter som rapporterats in till myndigheten[65] enligt NIS-lagen.[66]

2.3.2 IMY ska ge vägledning för skydd av personuppgifter och utöva tillsyn inom alla sektorer

IMY:s uppdrag är att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter, och för att underlätta det fria flödet av sådana uppgifter inom EU.[67] Uppdraget innebär att dels vidta åtgärder för att förebygga överträdelser av förordningen och genom tillsyn se till att förordningen följs, dels säkerställa att man varken ställer upp högre eller lägre krav på aktörerna än motsvarande systermyndigheter inom EU.

I likhet med andra tillsynsmyndigheter enligt dataskyddsförordningen regleras IMY:s uppgifter i artikel 57.1 i dataskyddsförordningen. IMY har i uppdrag att ge vägledning till verksamheter i alla samhällssektorer, offentlig som privat verksamhet, när det gäller att skydda personuppgifter vid behandling.[68] Inom ramen för det vägledande uppdraget ska IMY vidta åtgärder för att höja verksamheters medvetenhet om sina skyldigheter enligt dataskyddsförordningen.[69] Syftet är att verksamheter ska behandla och skydda personuppgifter på ett korrekt sätt enligt dataskyddsförordningen och kompletterande lagstiftning, till exempel PDL.[70] IMY ska också ge råd till en verksamhet vid behandling av personuppgifter[71] som den personuppgiftsansvarige bedömt kan leda till en hög risk för de registrerade efter genomförd konsekvensbedömning (så kallat förhandssamråd).[72] IMY ska även delta i och bidra till Europeiska dataskyddsstyrelsens arbete. Syftet är bland annat att ta fram vägledning till verksamheter.[73]

---

64 11 b § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap.

65 11 a § förordningen med instruktion för Myndigheten för samhällsskydd och beredskap.

66 De aktörer som levererar samhällsviktiga och digitala tjänster är vårdgivare och apotek. 12 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster och bilaga 1 Europaparlamentets och rådets förordning (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

67 1 § förordningen med instruktion för Integritetsskyddsmyndigheten.

68 Artikel 57.1 b, c, e och t samt artikel 58.3 a dataskyddsförordningen.

69 Artikel 57.1 d dataskyddsförordningen.

70 IMY:s svar på skriftliga frågor, 2023-10-04.

71 Med behandling av personuppgifter avses åtgärder såsom lagring, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt.

72 Artikel 36. 2 och artikel 57.1 l dataskyddsförordningen.

73 2a § förordningen med instruktion för Integritetsskyddsmyndigheten. Se även se artikel 57.1 t dataskyddsförordningen.

IMY är även mottagare av anmälningspliktiga personuppgiftsincidenter i organisationer som hanterar personuppgifter, bland annat vård- och omsorgsgivare i regioner och kommuner.[74]

IMY är tillsynsmyndighet för behandling av personuppgifter enligt dataskyddsförordningen[75] och kompletterande lagstiftning. IMY ska bedriva tillsyn över hur exempelvis vård- och omsorgsgivarna tillämpar dataskyddsbestämmelser,[76] vilket innebär att IMY till exempel kan kontrollera att de vidtar säkerhetsåtgärder för att skydda känsliga personuppgifter.

IMY ska vara oberoende i utförandet av sina uppgifter och i utövandet av sina befogenheter i enlighet med dataskyddsförordningen.[77] Kravet på att IMY ska vara oberoende innebär både att myndigheten ska vara fristående och självständig i förhållande till den verksamhet som den är satt att övervaka och att det inte får förekomma någon påverkan eller några instruktioner, direkt eller indirekt, från något annat håll, såsom från staten.[78] IMY:s oberoende innebär dock inte att dess uppgifter inte kan underkastas kontroll- och övervakningsmekanismer eller bli föremål för domstolsprövning.[79]

2.3.3 Socialstyrelsen ska normera och stödja vårdens och omsorgens informationssäkerhet

Socialstyrelsen är den kunskapsstyrande myndigheten för verksamhet som rör hälso- och sjukvård och socialtjänst. Socialstyrelsens ansvar gäller i den utsträckning sådana frågor inte ska handläggas av någon annan myndighet. Socialstyrelsen ansvarar för föreskrifter och allmänna råd inom sitt verksamhetsområde. Socialstyrelsen ansvarar också för kunskapsutveckling och kunskapsförmedling inom sitt område.[80]

Socialstyrelsen får meddela föreskrifter om verkställigheten av PDL.[81] De föreskrifterna omfattar hälso- och sjukvårdens informationshantering, det vill säga vårdgivares behandling och skydd av individers personuppgifter. Socialstyrelsen får även meddela föreskrifter om socialtjänstens behandling och dokumentation av individers personuppgifter.[82] Socialstyrelsen får också meddela föreskrifter enligt NIS-lagen om vårdgivarnas informationssäkerhet[83] och personuppgiftshantering

74 Artikel 33, dataskyddsförordning.
75 2 a § förordningen med instruktion för Integritetsskyddsmyndigheten.
76 Artikel 51.1 dataskyddsförordningen.
77 Artikel 52.1 dataskyddsförordningen. Se även mejl från företrädare för IMY, 2022-12-07.
78 Artikel 52.2 dataskyddsförordningen, SOU 2016:65 s. 144 och EU-domstolens dom C-518/07.
79 Artikel 78 dataskyddsförordningen. Skäl 118.
80 1 och 4 §§ förordningen med instruktion för Socialstyrelsen.
81 2 och 3 §§ patientdataförordningen. Bemyndigandet framgår även av 4 kap. 2 § patientdatalagen samt när det gäller kontroll av elektronisk åtkomst till patientuppgifter med stöd av sin s.k. restkompetens, se 4 kap 3 § sista stycket patientdatalagen. 26 § förordning (2001:637) om behandling av personuppgifter inom socialtjänsten. IMY ska få möjlighet att yttra sig innan Socialstyrelsen får meddela föreskrifter.
82 7 b § lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, 26–27 §§ förordningen om behandling av personuppgifter inom socialtjänsten.
83 8 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster

enligt lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation som rör bland annat krav på säkerhetsåtgärder som ska gälla vid direktåtkomst eller annat elektroniskt utlämnande och tilldelning av behörighet för åtkomst till uppgifter.[84] Socialstyrelsen är även mottagare av IT-incidentrapportering från leverantörer inom hälso- och sjukvård.[85]

2.3.4 IVO ska bedriva tillsyn av vårdens och omsorgens informationssäkerhet

IVO är tillsynsmyndighet för hälso- och sjukvård och omsorg. Syftet med tillsynen är att granska att befolkningen får vård och omsorg som är säker, har god kvalitet och bedrivs i enlighet med lagar och andra föreskrifter. IVO:s tillsyn ska vara riskbaserad och bedrivas strategiskt och effektivt samt på ett enhetligt sätt inom landet.[86]

Sedan 1 augusti 2018 ansvarar IVO för tillsyn av informationssäkerhet i hälso- och sjukvården enligt NIS-lagen.[87] Tillsynsuppdraget omfattar tre områden: att identifiera och registrera de vårdgivare som omfattas av lagen[88], att ta emot incidentrapporter från vårdgivare och att bedriva tillsyn av vårdgivare. IVO ska utan dröjsmål delge MSB uppgifter om de vårdgivare som man identifierat omfattas av lagen.[89]

Tillsynen enligt NIS-lagen omfattar vårdgivarnas skyldighet att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete avseende nätverk och informationssystem i syfte att uppnå en hög säkerhetsnivå. Det omfattar vårdgivarnas ansvar att ta fram riskanalyser och åtgärdsplaner, vidta ändamålsenliga och proportionerliga tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem samt vidta åtgärder för att förebygga och minimera verkningar av incidenter som kan påverka kontinuiteten i systemen.[90] IVO ska också inom ramen för tillsynen enligt NIS-lagen ge allmän vägledning i tillämpningen av lagen.[91]

IVO kan i sin tillsyn av vården och omsorgen även utgå från annan lagstiftning än NIS-lagen som berör skyddet av personuppgifter, såsom PDL och lagen om behandling av personuppgifter inom socialtjänsten. IVO ska samverka med andra berörda myndigheter i syfte att uppnå ett effektivt kunskaps- och erfarenhetsutbyte i

84 Se även 27 § förordningen om behandling av personuppgifter inom socialtjänsten.
85 12 § förordningen om informationssäkerhet för samhällsviktiga och digitala tjänster.
86 1–2 §§ förordningen med instruktion för Inspektionen för vård och omsorg.
87 17 § NIS-förordningen.
88 I NIS-lagen används termen *leverantör* av samhällsviktiga tjänster. Inom hälso- och sjukvården är leverantörerna vårdgivare. Med vårdgivare avses en statlig myndighet, region och kommun i fråga om sådan hälso- och sjukvårdsverksamhet som myndigheten, regionen eller kommunen har ansvar för (offentlig vårdgivare) samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet (privat vårdgivare), MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9).
89 19 § 1 st. NIS-förordningen.
90 11–16 §§ NIS-lagen.
91 19 § NIS-förordningen.

arbetet med tillsyn, styrning med kunskap och regelgivning.[92] IVO ska delta i ett samarbetsforum för tillsynsmyndigheter enligt NIS-lagen med syfte att samordna tillsynen och åstadkomma en effektiv och likvärdig tillsyn.[93] IVO ska också samarbeta med IMY vid hantering av incidenter som även utgör personuppgiftsincidenter.[94]

IVO är liksom Socialstyrelsen mottagare av information om de IT-incidenter som leverantörer inom hälso- och sjukvården enligt NIS-lagen ska rapportera till MSB.[95]

2.3.5 Överenskommelser mellan regeringen och SKR

SKR har inom ramen för överenskommelser med regeringen ett visst ansvar för att ge vården och omsorgen stöd för informationssäkerhet. SKR driver också nätverk för informationssäkerhet i regioner och kommuner,[96] och har tagit fram ett verktyg för klassificering av information som ska skyddas i vård och omsorg kallat Klassa.

Regeringen och SKR slöt i februari 2020 en överenskommelse[97] för att stödja kommunernas arbete med att införa välfärdsteknik i äldreomsorgen. Satsningen omfattade riktade medel och en samordnande stödfunktion och gällde från 2020 till 2022. Medlen för 2023 beviljades av regeringen efter en ansökan.[98] Av totalt 200 miljoner kronor per år gick cirka 17 miljoner kronor till SKR för att stödja kommunerna medan resten fördelades som statsbidrag till kommunerna. Inom denna överenskommelse skulle SKR stödja kommunernas arbete med att digitalisera äldreomsorgen och ge råd, stöd och vägledning i frågor om bland annat informationssäkerhet. Flera andra överenskommelser mellan regeringen och SKR omfattar indirekt informationssäkerhet.[99]

2.4 Brister i regioners och kommuners informationssäkerhet

Det finns sammantaget relativt god kunskap på nationell nivå om brister i regioners och kommuners informationssäkerhetsarbete. Flera myndigheter har i uppdrag att följa utvecklingen av informationssäkerhet och den incidentrapportering som verksamheter är skyldiga att göra.

92 4 § förordningen med instruktion för Inspektionen för vård och omsorg.
93 21 § NIS-förordningen.
94 19 § 4 st. NIS-förordningen.
95 12 § NIS-förordningen.
96 Hälso- och sjukvårdens informationssäkerhetsnätverk (HoSIS) och Informationssäkerhetsnätverket Sveriges Kommuner (KIS).
97 Regeringsbeslut 2020/00577/SOF.
98 Regeringsbeslut S2023/00101.
99 Ett exempel är en överenskommelse som slöts 2023 om att stärka hälso- och sjukvårdens arbete med civilt försvar, regeringsbeslut S2023/00374. Regionerna ska tilldelas totalt 405 miljoner kronor under 2023 för att bland annat stärka förmågan att motstå cyberangrepp i vårdens digitala system. SKR ska också ge praktiskt stöd till regionerna i detta arbete. SKR och regionerna ska lämna en redovisning till Socialstyrelsen senast den 31 mars 2024. Andra exempel är regeringsbeslut S2017/00378, S2019/03011, S2021/00820 (delvis), S2021/08204, S2021/02919.

2.4.1 Alla regioner och kommuner arbetar inte systematiskt med informationssäkerhet

Uppföljningar av informationssäkerhet visar att stora delar av den offentliga förvaltningen inte bedriver ett effektivt informationssäkerhetsarbete. Det gäller särskilt kommuner, även om spridningen mellan kommunerna är stor.

Enligt MSB arbetar stora delar av den offentliga förvaltningen inte systematiskt med informationssäkerhet. Det finns ett starkt fokus på att implementera säkerhetsåtgärder, men det finns brister i arbetet med att bedöma risker och implementera säkerhetsåtgärderna så att de ger tillräckligt skydd utifrån de identifierade riskerna. Dessutom är uppföljningen av införda säkerhetsåtgärder ofta otillräcklig.[100] IVO ger en liknande bild när det gäller vården. Vissa vårdgivare brister i att utföra och uppdatera riskanalyser samt upprätta åtgärdsplaner, särskilt vid uppdatering av journalsystem, vilket ökar risken för att de inte genomför tillräckliga säkerhetsåtgärder.[101]

Informationssäkerhetsarbetet är mest eftersatt i kommunerna. Exempelvis uppnådde 3 av 4 kommuner som deltog i MSB:s Infosäkkoll 2023 inte den mest grundläggande nivån i det systematiska informationssäkerhetsarbetet. (Se avsnitt 3.1.1 för mer om skattningsverktyg Infosäkkollen.) MSB har bedömt att en majoritet av kommunerna inte avsätter tillräckligt med resurser för informationssäkerhetsarbetet och att ledningarna sällan informerar sig om vilka övergripande informationssäkerhetsrisker kommunen har. En majoritet av kommunerna är dåligt förberedda om något allvarligt skulle hända. Men det finns stora skillnader mellan kommunerna.[102]

Det finns samtidigt tecken på en positiv utveckling enligt en undersökning från Socialstyrelsen. Exempelvis ökade andelen kommuner som har infört ledningssystem för informationssäkerhet från 43 till 49 procent mellan 2021 och 2023. Andelen kommuner som följt upp risker för informationssäkerhet i socialtjänsten ökade under samma period från 48 till 60 procent, och andelen som gjort det i kommunal vård ökade från 40 till 58 procent mellan 2022 och 2023. Socialstyrelsen bedömer samtidigt att många kommuner saknar delar i sitt informationssäkerhetsarbete och menar att ett utökat nationellt stöd kan främja utvecklingen, framför allt om det riktas till mindre kommuner som inte har kommit lika långt som större.[103]

Regionerna har enligt MSB generellt en högre nivå på sitt informationssäkerhetsarbete än kommunerna, men i Infosäkkollen 2023 var det 67 procent av 18 regioner som inte nådde den mest grundläggande säkerhetsnivån. Det finns exempelvis brister i regionernas kunskap om vilken information och vilka

---

100 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen*, 2024. MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, 2022, s. 8.

101 IVO, *Vad har IVO sett 2020?* 2021, s. 88–89.

102 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen,* 2024. MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, 2022, s. 19–26.

103 Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2023,* 2023, s. 77.

informationssystem som finns den egna verksamheten. Det finns även brister i uppföljningen av om krav som ställts i samband med upphandlingar varit tillräckliga och om den kontrakterade parten har infört de säkerhetsåtgärder som avtalats.[104]

2.4.2 Låg prioritet och brist på kompetens och resurser är viktiga orsaker till brister i informationssäkerhet

De huvudsakliga orsakerna till bristande informationssäkerhet, särskilt i kommunerna, är att verksamheternas ledningar inte prioriterat informationssäkerhetsarbetet och brist på resurser och kompetens.

Att många verksamheter inte arbetar systematiskt med informationssäkerhet är ofta kopplat till verksamhetsledningen. MSB lyfter fram att ledningens frånvaro är en brist, särskilt i kommunerna. Ledningarna informerar sig inte om kommunens övergripande risker och fattar inte beslut om att hantera risker som kan få stor påverkan på verksamheten. Därmed riskerar informationssäkerhetsarbetet att nedprioriteras. Enligt MSB behöver kommunerna utbildning i informationssäkerhet för att kunna utveckla sitt informationssäkerhetsarbete.[105] Enligt IVO är verksamhetsledningens ansvar hos vårdgivare ofta otydligt. Mandat och befogenheter är oklara, ansvaret för samverkan mellan olika verksamhetsdelar är otydligt och det saknas dokumenterade arbetssätt. Det kan leda till att risker inte upptäcks och säkerhetsåtgärder inte genomförs i tid.[106]

Otillräckliga resurser och ineffektivitet är två andra betydande orsaker till brister i informationssäkerhetsarbetet. Enligt MSB:s Infosäkkollen identifierar många verksamheter brist på resurser som det främsta hindret för att förbättra sitt informationssäkerhetsarbete. Särskilt kommuner behöver tillföra mer resurser enligt MSB, samtidigt som myndigheten betonar att det finns utrymme för att öka effektiviteten i arbetet för att frigöra resurser för att stärka informationssäkerhetsarbetet. MSB bedömer dock att endast ett fåtal verksamheter kommer att tillföra tillräckligt med resurser för att stärka informationssäkerheten.[107]

En annan betydande orsak till bristande informationssäkerhet är bristen på personal med rätt kompetens och låg kunskapsnivå hos de som arbetar med informationssäkerhet.[108]

---

104 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen,* 2022.

105 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen,* 2024. MSB, *Behovsanalys informationssäkerhet, upplevda hinder vid systematiskt informationssäkerhetsarbete,* 2023. MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen,* 2022.

106 IVO, *Vad har IVO sett 2020?*, 2021, s. 89.

107 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen,* 2024. MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen,* 2022.

108 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen,* 2024. MSB, *Behovsanalys informationssäkerhet, upplevda hinder vid systematiskt informationssäkerhetsarbete,* 2023. MSB:s svar på skriftliga frågor, 2023-10-06.

2.4.3 Vårdgivare står för en betydande andel av incidenter

Vård- och omsorgsgivare ska rapportera in personuppgiftsincidenter[109] till IMY, och vårdgivare som omfattas av NIS-lagen ska rapportera IT-incidenter[110] till MSB som ska dela dem med IVO och Socialstyrelsen. Incidentrapporteringen visar att en stor andel av incidenterna kommer från vårdgivare.

Under 2023 fick MSB in 145 incidentrapporter från NIS-leverantörer vilket är en ökning med 46 rapporter jämfört med 2022. Antalet rapporter från vården ökade med cirka 70 procent, vilket enligt MSB indikerar att antalet IT-incidenter inom sektorn har ökat. Omkring 30 procent av de inrapporterade incidenterna från vården bedöms ha haft en betydande eller en viss påverkan på människors hälsa.[111] Under 2021 och 2022 var den vanligaste orsaken till rapporteringen från vården att incidenten påverkat tillgängligheten till system. Under dessa år var det totalt 14 regioner och 27 kommuner som rapporterade in minst en incident.[112]

Under 2022 fick IMY in cirka 5 300 anmälningar om personuppgiftsincidenter, varav var femte gällde vårdgivare.[113] Totalt 73 procent av incidenterna gällde obehörigt röjande av personuppgifter genom felaktiga utskick exempelvis via mejl eller andra misstag,[114] och 19 procent uppstod genom obehörig åtkomst, till exempel genom felaktig tilldelning av behörigheter till IT-system. I 70 procent av fallen inom vården var den mänskliga faktorn orsak till incidenten.[115]

Ett syfte med rapporteringen är att ge myndigheterna kunskap om brister i informationssäkerhet. Det finns dock en stor underrapportering av incidenter, vilket gör det svårt att dra långtgående slutsatser om incidentrapporteringen. I kapitel 3 och 5 redogör vi för hur myndigheterna hanterar incidenterna.

---

109 En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats, det vill säga informationssäkerhet för information.

110 En incident är enligt 2 § NIS-lagen en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem. Hur incidentrapporteringen ska göras bestäms enligt 11–15 § NIS-förordningen.

111 MSB, *EU förändrar cybersäkerhetsområdet. Årsrapport it-incidentrapportering 2023*, 2024, s. 18, 31.

112 MSB:s svar på skriftliga frågor, 2023-10-06.

113 IMY, *Anmälda personuppgiftsincidenter 2022,* 2023.

114 Till exempel att personuppgifter avsiktligt eller oavsiktligt röjts för någon som saknar behörighet eller att brister i ett tekniskt system gjort att personuppgifter kommit till fel mottagare.

115 IMY, *Anmälda personuppgiftsincidenter 2022,* 2023, s. 23–27, 52.

3 Statens styrning av och stöd till vårdens och omsorgens informationssäkerhetsarbete

I detta kapitel besvaras den första delfrågan: Är myndigheternas arbete med att styra och stödja vårdens och omsorgens informationssäkerhetsarbete effektivt? Detta är våra viktigaste iakttagelser:

- MSB:s, IMY:s och Socialstyrelsens respektive stöd för informationssäkerhetsarbete är inte tillräckligt anpassat efter vård- och omsorgsgivarnas behov. Myndigheterna ger inte tillräckligt stöd för hur bestämmelserna för skydd av personuppgifter kan omsättas i det praktiska informationssäkerhetsarbetet, exempelvis vägledning om rutiner och rekommendationer för användning av IT-produkter.
- Socialstyrelsen och IMY tar sällan ställning i rättsliga frågor vilket begränsar utvecklingen av praxis och tydlig vägledning. En förklaring är att IMY och Socialstyrelsen är försiktiga med att tolka bestämmelserna.
- Socialstyrelsen har ännu inte tagit fram föreskrifter till NIS-lagen, vilket har bland annat begränsat stödet till vårdgivare och IVO:s tillsyn.
- Myndigheterna arbetar också i stuprör och har inte samverkat eller samordnat sina insatser när de utformar sitt stöd. Varken MSB, IMY eller Socialstyrelsen anser sig ha ansvar att utforma stöd som är anpassat efter vård- och omsorgsgivares behov, vilket fördröjer ett effektivt arbete.
- Regeringens åtgärder för att stärka vårdens och omsorgens informationssäkerhet har inte varit tillräckliga. Regeringen har inte tydligt fastställt ansvars- och uppgiftsfördelningen mellan IMY, MSB och Socialstyrelsen när det gäller att utforma stöd som motsvarar vårdgivares och omsorgsgivares behov. Regeringen har inte heller sett till att myndigheterna samordnar sitt arbete med stödet.
- Trots att omsorgen ofta hanterar lika känsliga personuppgifter som vården, har regeringen inte verkat tillräckligt för att omsorgsgivare ska omfattas av samma tydliga krav på säkerhetsåtgärder och systematiskt informationssäkerhetsarbete som vårdgivare, förutom när det gäller viss behörighetstilldelning och kontroll av behörigheterna.

3.1 MSB ger generellt stöd för systematiskt informationssäkerhetsarbete

MSB:s stöd för informationssäkerhetsarbete är uppskattat eftersom det vägleder verksamheter när de ska bygga upp det systematiska informationssäkerhetsarbetet. Men stödet är inte tillräckligt konkret när det gäller hur en verksamhet kan göra i praktiken för att skydda personuppgifter. Stödet är inte anpassat efter vårdens och

omsorgens behov eftersom MSB inte anser att de har i uppdrag att ta fram sektorsspecifikt stöd. Enligt MSB är det Socialstyrelsen som har detta uppdrag inom vården och omsorgen. MSB har följt upp det egna stödet men det har inte lett förändringar av stödet. För att motverka sårbarheter sprider MSB information om risker och hot mot informationssäkerheten via olika kanaler till regioner och kommuner, men får viss kritik för att informationen inte alltid är tillräckligt konkret att agera på. MSB tar fram föreskrifter för systematiskt informationssäkerhetsarbete, men föreskriftsrätten omfattar inte vården och omsorgen utöver de vårdgivare som omfattas av NIS-lagen.

3.1.1 MSB:s stöd är uppskattat men inte anpassat till vården och omsorgen

MSB:s stöd för informationssäkerhet används och är uppskattat av vård- och omsorgsgivare. Men stödet är inte tillräckligt konkret och anpassat efter deras behov eftersom MSB inte anser att de har i uppdrag att utveckla anpassat stöd för olika sektorer.

MSB har ett brett uppdrag att ge generellt stöd för systematiskt informationssäkerhetsarbete och MSB:s stödmaterial, utbildningar och stödfunktioner är utvecklade för att passa alla typer av verksamheter. Ett centralt stödmaterial är MSB:s metodstöd för systematiskt informationssäkerhetsarbete som bygger på internationella standarder, och inte tagits fram utifrån en enskild lagstiftning.[116] Det ska ge ett praktiskt stöd till verksamheter att komma i gång med och förbättra alla delar i sitt informationssäkerhetsarbete och ska kunna användas oavsett hur långt verksamheten kommit i arbetet.[117] Som komplement till metodstödet har MSB tagit fram vägledningar, stödmaterial och informationsfilmer samt ger råd via en upplysningstjänst. MSB ordnar också utbildningar och webbutbildningar och har tagit fram ett självskattningsverktyg för återkoppling och uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, kallat Infosäkkollen.[118]

Vård- och omsorgsgivare tar del av och använder MSB:s stöd, men stödet är inte anpassat för verksamheter inom vården och omsorgen. Stödet talar framför allt om vad en verksamhet behöver göra inom ramen för det systematiska informationssäkerhetsarbetet, men inte hur den i praktiken kan göra för att skydda personuppgifter utifrån sina arbetssätt och sina informationssystem, vilket särskilt mindre kommunala vård- och omsorgsgivare har behov av.

MSB anser att det inte ingår i deras uppdrag att utveckla stöd som är anpassade efter olika sektorers behov. MSB anser att Socialstyrelsen har ansvaret för att ge specifikt stöd till vård- och omsorgsgivares informationssäkerhetsarbete. MSB menar också att

116 Det baseras på standarderna SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002.
117 MSB, *Metodstöd för systematiskt informationssäkerhetsarbete – En översikt,* 2021.
118 Enligt regeringsuppdrag, Regeringsbeslut Ju2019/03058/SSK Ju2019/02421/SSK.

deras resurser inte räcker till för att anpassa befintligt stöd efter alla specifika målgruppers behov, även om de skulle haft ett sådant uppdrag. MSB saknar dessutom kunskap om vård- och omsorgsgivares förutsättningar för att veta om och hur stödet behöver anpassas.[119]

I avsnitten nedan utvecklar vi våra iakttagelser av MSB:s olika stöd.

Metodstödet är inte sektorsspecifikt

MSB:s metodstöd för att bygga upp och bedriva ett systematiskt informationssäkerhetsarbete är uppdelat i fyra steg: identifiera och analysera, utforma, använda samt följa upp och förbättra. Stegen innebär bland annat att verksamheten ska analysera och identifiera risker och den egna verksamhetens behov, ta fram interna styrdokument och handlingsplaner, implementera olika säkerhetsåtgärder, till exempel klassning av information och utbildning av personal, samt följa upp åtgärderna och genomföra förbättringar.[120]

Metodstödet används och är uppskattat enligt de intervjuer som vi genomfört med kommuner och regioner. Det framkommer även i en uppföljning av stödet som MSB låtit genomföra.[121] En generell synpunkt som framkommer i flera intervjuer med kommuner är att MSB tar sin stödjande roll på allvar och upplevs vilja hjälpa till med att stärka deras informationssäkerhetsarbete.[122] Metodstödet upplevs framför allt som konkret när det gäller vad det systematiska informationssäkerhetsarbetet ska innehålla. Det får samtidigt kritik i en del intervjuer för att det ger för lite konkret vägledning i hur man ska göra när stödet ska omsättas i praktiken, till exempel vad en relevant säkerhetsåtgärd är eller hur man ska tänka när man gör en riskanalys för den egna verksamheten.[123] Motsvarande bild framkom i MSB:s uppföljning av metodstödet. Metodstödet är lättare att använda för verksamheter med stora resurser eftersom det kräver tid och kompetens, medan mindre verksamheter har ett behov av mer stöd för hur informationssäkerhetsarbetet ska implementeras.[124] Vår granskning visar att metodstödet inte upplevs vara tillräckligt anpassat för vårdens och omsorgens behov. Ett exempel som lyfts fram är konkret stöd i vilka risker som finns för skydd av uppgifter inom vården.[125]

Enligt MSB är metodstödet inte tänkt att ge stöd i specifika frågor utan bygger på att en verksamhet arbetar systematiskt och riskbaserat genom att identifiera vilka säkerhetsåtgärder de behöver implementera. MSB kan inte ge specifikt stöd eftersom det ser väldigt olika ut i olika sektorer, inom olika organisationer och i olika IT-system som organisationer använder sig av. Det gör att en verksamhet själv exempelvis måste

---

119 Intervju med företrädare för MSB, 2023-05-11, 2022-12-12 och 2022-12-16.
120 MSB, *Metodstöd för systematiskt informationssäkerhetsarbete – En översikt,* 2021.
121 MSB, *Utvärdering av metodstöd,* 2022.
122 Intervju med företrädare för kommun 1, kommun 2 och kommun 3.
123 Intervju med företrädare för region 1, region 2, kommun 4 och kommun 6. Se även intervju med företrädare för SKR, 2023-06-08.
124 MSB, *Utvärdering av metodstöd,* 2022.
125 Intervju med företrädare för kommun 1.

identifiera vilka risker den har och utgå från dem. Det innebär också att MSB inte kan ge specifika råd om exempelvis vilka behörigheter som ska tilldelas, vilka kontroller av loggar som ska genomföras eller vilka brandväggar man ska ha för att skydda information.[126] MSB kan exempelvis ge råd om hur man ska tänka inför behörighetstilldelning, men inte om hur många behörighetsgrupper som behövs eller vilka behörigheter som olika yrkesgrupper eller enskilda personer ska tilldelas.[127]

Rådgivningstjänsten ger inte råd om specifika åtgärder

För att komplettera metodstödet, vägledningar och annat stödmaterial har MSB sedan hösten 2022 en rådgivningstjänst som ska ge stöd till verksamheters systematiska informationssäkerhetsarbete. Syftet är att hjälpa olika verksamheter att anpassa sitt informationssäkerhetsarbete utifrån MSB:s stöd.[128] Vår genomgång av frågorna till tjänsten under hösten 2022 visar att den sällan ger råd om vilka specifika åtgärder som ska genomföras. Kommuner och regioner blir oftast hänvisade till MSB:s vägledningar och stödmaterial. Majoriteten av frågorna kom från kommunerna och handlade om hur man ska bygga ett systematiskt informationssäkerhetsarbete och hur man ska införa säkerhetsåtgärder i den egna verksamheten.[129]

Infosäkkollen är anpassad för verksamheter med mindre utvecklat informationssäkerhetsarbete

MSB har inom ramen för ett regeringsuppdrag om att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen utvecklat ett digitalt verktyg, Infosäkkollen. Det är ett frivilligt självskattningsverktyg som ska ge verksamheter en bild av nivån på sitt informationssäkerhetsarbete och ge förslag på förbättringsåtgärder. Ett syfte är även att verktyget ska ge MSB underlag för att regelbundet ge regeringen en samlad bedömning av nivån på det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.[130] Undersökningen har genomförts 2021 och 2023. Under 2023 var svarsfrekvensen 86 procent för regioner och 53 procent för kommuner. Under 2023 tillkom frågor om säkerheten i IT-system och det blev möjligt att jämföra det egna resultatet med sammanställda resultat från samtliga deltagande verksamheter.[131]

I vår granskning framkommer att Infosäkkollen är uppskattad av de som använder verktyget[132] vilket också är MSB:s bild, men verktyget får viss kritik för att inte ge tillräcklig konkret vägledning för verksamheter som kommit längre i sitt informationssäkerhetsarbete. MSB har medvetet valt att utforma Infosäkkollen så att

126 Intervju med företrädare för MSB, 2023-05-11.
127 E-post från MSB, 2024-02-12.
128 MSB, ”Rådgivningstjänst för systematiskt informationssäkerhetsarbete”, hämtad 2023-05-08.
129 Se bilaga 2 för mer om inkomna frågor till MSB.
130 Regeringsbeslut 2019-09-19, Ju2019/03058/SSK, Ju2019/02421/SSK.
131 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen,* 2024.
132 Intervju med företrädare för kommun 2 och kommun 6.

den ger återkoppling på en relativt grundläggande nivå för att verktyget ska kunna användas av och fungera för alla typer av verksamheter.[133]

Att Infosäkkollen är frivilligt att använda och att verktyget framför allt är anpassat för verksamheter som inte kommit så långt i sitt informationssäkerhetsarbete påverkar dess svarsfrekvens. Det försvagar MSB:s uppföljning av nivån på det systematiska informationssäkerhetsarbetet och den rapportering som MSB gör till regeringen.

Exempelvis pekar MSB på att en viss förbättring i informationssäkerhet som kan ses mellan 2021 och 2023 delvis är svårtolkad eftersom deltagandet av mer utvecklade verksamheter ökade medan det minskade för verksamheter som hade sämre resultat 2021. Enligt MSB bör det vara obligatoriskt för offentlig förvaltning och NIS-leverantörer att delta i Infosäkkollen.[134]

Utbildningar riktas inte längre till kommunledningar

En viktig faktor för att utveckla informationssäkerhetsarbetet i en verksamhet är att dess ledningsfunktioner har intresse för och kunskap om frågan, något som MSB har identifierat som en vanlig brist i kommunerna.[135] MSB genomför inga utbildningar som riktas till kommuners och regioners ledningar.

MSB har tagit fram olika webbutbildningar för att stärka arbetet med informationssäkerhet och har på uppdrag av regeringen tagit fram och genomfört olika kompetenshöjande utbildningar om informationssäkerhet för personal i offentlig sektor.[136] Inom ramen för regeringsuppdrag[137] har MSB tidigare genomfört utbildningar för CISO (”chief information security officer”) och ledningar i kommuner, regioner och statliga myndigheter men lade ner kursen eftersom den inte nådde personer i ledande ställning och inte ansågs vara resurseffektiv. MSB har inga utbildningar för kommunala eller regionala ledningsfunktioner inplanerade, men undersöker möjligheten att nå målgruppen till exempel via mindre resurskrävande webbutbildningar och i samarbete med SKR.[138]

MSB:s stöd finns på olika webbsidor

MSB publicerar stödmaterial för informationssäkerhet på olika webbsidor och det är inte alltid uppdaterat. Det gör att stödet delvis brister i tillgänglighet.

MSB publicerar för närvarande sina vägledningar och annat stödmaterial på tre olika webbplatser vilket kan skapa viss förvirring. Det finns även kritik mot att vägledningar och stöd på webbsidorna inte är uppdaterade och att inaktuella versioner kommer fram vid sökningar.[139] Att inaktuella versioner dyker upp kan

133 Intervju med företrädare för MSB, 2023-02-20.
134 MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen,* 2024.
135 MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen,* 2022.
136 Regeringsbeslut 2018-04-12 Ju2018/02265/SSK. Regeringsbeslut 2019-09-19 Ju2019/03057/SSK.
137 Regeringsbeslut Ju2018/02265/SSK och Ju2019/03057/SSK.
138 MSB:s svar på skriftliga frågor, 2023-10-06.
139 Intervju med företrädare för MSB, 2022-12-12.

enligt MSB bero på MSB:s interna versionshantering och på att sökmotorer söker upp vägledningar som funnits länge eftersom de är de mest eftersökta. En annan synpunkt är att en vägledning plötsligt kan tas bort utan information om varför.[140] MSB arbetar med att samla allt stödmaterial till sin webbplats för att öka tillgängligheten.

3.1.2 Informationsspridningen om risker och hot får viss kritik

MSB har i uppdrag att sprida information om hot och sårbarheter i IT-system som skyddar information via sin CERT-funktion, som även ska ge operativt stöd vid IT-incidenter (se avsnitt 3.4.1). CERT-funktion sprider information om risker och hot mot informationssäkerhet till regioner och kommuner men får viss kritik för att informationen inte alltid är tillräckligt konkret för att vara möjlig att agera på.

CERT-funktionen sprider informationen genom webbpubliceringar eller så kallade blixtmeddelanden (prenumerationstjänst)[141] och via riktade säkerhetsmeddelanden till organisationer med bland annat en identifierad sårbarhet.[142] Under 2022 publicerade MSB 156 webbartiklar med information om sårbarheter, hot och risker med rekommendationer och gjorde 900 utskick av säkerhetsmeddelanden.[143] Inom vården sprids information till regionerna via Hälso- och sjukvårdens informationssäkerhetsnätverk (HOSIS) och till kommunerna via Informationssäkerhetsnätverket Sveriges kommuner (KIS). Information sprids även i Forum för informationsdelning för privat och offentlig samverkan (Fidi).[144]

I våra intervjuer framkommer både positiva och negativa omdömen om MSB:s information om risker och hot. MSB får viss kritik för att informationen är för allmängiltig för att den ska gå att agera på, men uttrycker förståelse för att den inte kan vara för specifik av sekretesskäl.[145] En kommun upplever informationen från MSB som konkret och värdefull.[146]

MSB har utvecklat CERT-funktionen inom ramen för ett regeringsuppdrag som avrapporterades under 2023. MSB tog fram nya digitala verktyg för incidentrapportering och delning av sårbarhetsinformation samt en plattform för att dela information om indikatorer på dataintrång, men uppger att man behöver fortsatt utveckla sina förmågor att skaffa kunskap om hot och att kunna upptäcka intrång i realtid för att avvärja dem.[147] Regeringen har tillfört MSB 20 miljoner kronor under 2024 för att utveckla CERT-funktionen.[148]

---

140 Intervju med företrädare för region 1.
141 Prenumerationstjänsten når ut till 16 000 prenumeranter.
142 MSB:s svar på skriftliga frågor, 2023-10-06.
143 MSB, *Årsredovisning 2022*, 2023.
144 MSB:s svar på skriftliga frågor, 2023-10-06.
145 Intervju med företrädare för region 1.
146 Intervju med företrädare för kommun 1.
147 MSB, Redovisning av regeringsuppdrag Ju2022/02219, 2023.
148 Prop. 2023/24:1 Utgiftsområde 6, s. 96.

3.1.3 MSB har följt upp det egna stödet men analyserar inte mörkertalet av IT-incidenter

MSB följde 2022 upp sitt metodstöd och genomförde 2023 en behovsanalys av vilka hinder som finns för att höja nivån på det systematiska informationssäkerhetsarbetet inom bland annat regioner och kommuner. Syftet var att få underlag för utveckling av stödet.[149] Resultatet från 2022 visade bland annat att regioner och kommuner efterfrågade mer konkret och anpassat stöd när det gäller hur informationssäkerhet ska implementeras i organisationen. Enligt MSB visade uppföljningarna inte på några överraskande resultat utöver det som MSB redan kände till och resultatet har inte gett myndigheten anledning att förändra sin planering eller sina prioriteringar i utvecklingen av stödet.[150]

Vård- och omsorgsverksamheter ska rapportera in IT-incidenter till MSB och rapporterna utgör ett underlag för MSB:s analyser av brister i informationssäkerhet i olika verksamheter. Men det finns stor en underrapportering av incidenter och det är enligt MSB bara en tredjedel av alla inträffade incidenter som inrapporteras.[151] En stor andel av regionerna och kommunerna har inte rapporterat in någon incident under 2021 och 2022 (se avsnitt 2.4.3). Regeringen har uppmärksammat att underrapporteringen är ett problem eftersom rapporteringen är viktig för att kunna inrikta arbetet med att utveckla informationssäkerheten.[152]

En förklaring till underrapporteringen är enligt MSB att en incident ska vara betydande för att rapporteras in. När incidenten inte har lett till någon skada ser en verksamhet ingen anledning att anmäla incidenten, och när det som lett till en incident har lösts blir mervärdet av att anmäla också lägre.[153]

MSB har inte genomfört mörkertalsanalyser av varför rapporteringsfrekvensen skiljer sig åt mellan kommuner och regioner och varför vissa verksamheter inte alls rapporterar in några IT-incidenter.[154] Det är därför oklart om incidentanmälningarna ger en korrekt bild av problemen i vårdens och omsorgens informationssäkerhet. Som nämnts (se avsnitt 3.1.1) påverkar även utformningen av Infosäkkollen MSB:s uppföljningar. Det finns därmed flera svagheter i MSB:s underlag för uppföljning som påverkar MSB:s möjligheter att dra slutsatser om informationssäkerhetsbrister i bland annat vården och omsorgen. Det påverkar i sin tur MSB:s rapportering till regeringen om informationssäkerhetsbristerna.

---

149 MSB, *Utvärdering av metodstöd,* 2022 och MSB, *Behovsanalys informationssäkerhet, upplevda hinder vid systematiskt informationssäkerhetsarbete,* 2023. De huvudsakliga resultaten av uppföljningarna har beskrivits i avsnitt 2.4 och i avsnitt 3.1.1.

150 Intervju med företrädare för MSB, 2023-05-11.

151 MSB, *En inblick i Sveriges cybersäkerhet: Årsrapport IT-incidentrapportering 2021,* 2022. Intervju med företrädare för MSB, 2023-03-16.

152 Prop. 2022/23:1 Utgiftsområde 6, s. 86.

153 Intervju med företrädare för MSB, 2023-03-16.

154 Intervju med företrädare för MSB, 2023-02-20.

3.1.4 Krav på systematiskt informationssäkerhetsarbete omfattar inte omsorgen och mindre vårdgivare

MSB har föreskriftsrätt för systematiskt informationssäkerhetsarbete utifrån olika bestämmelser. MSB saknar lagstöd för att meddela föreskrifter för kommuners och regioners informationssäkerhetsarbete och de föreskrifter som MSB har tagit fram till NIS-lagen omfattar inte omsorgsgivare och mindre vårdgivare.

MSB har tagit fram föreskrifter om informationssäkerhet för statliga myndigheter och föreskrifter om säkerhet i informationssystem med tillhörande vägledning.[155] MSB har inte lagstöd för att ta fram motsvarande föreskrifter för kommuner och regioner, men rekommenderar regioner och kommuner att utgå från föreskrifterna och vägledningen för statliga myndigheter eftersom de också behöver bedriva ett systematiskt informationssäkerhetsarbete. Föreskrifterna är dock inte bindande för regioner och kommuner och kan därför bland annat inte utgöra grund för tillsyn. MSB önskar att få föreskriftsrätt för kommuners och regioners informationssäkerhet.[156]

MSB har även gett ut tre föreskrifter till NIS-lagen. MSB:s föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster ställer krav på de flesta vårdgivare att bedriva systematiskt informationssäkerhetsarbete, men de omfattar inte omsorgsgivare och de mindre vårdgivare som inte omfattas av NIS-lagen.

3.2 IMY ger generellt stöd för skydd av personuppgifter

IMY:s stöd till vård- och omsorgsgivarnas arbete med att skydda personuppgifter är generellt och inte anpassat efter deras behov. IMY ger inte specifikt stöd eftersom de inte anser att det ingår i deras uppdrag ta fram sektorsspecifikt stöd. Till exempel ger IMY sällan stöd för hur bestämmelserna som gäller för vården och omsorgen kan tolkas, vilket försvårar för vård- och omsorgsgivare att förstå vad som förväntas av dem. Vård- och omsorgsgivare kan söka råd från IMY för att hantera höga risker innan de påbörjar en personuppgiftsbehandling, men IMY ger dem inte tillräckligt stöd om hur de kan hantera riskerna. IMY:s tillsynsbeslut inom vården och omsorgen är svåra att använda som vägledning för skydd av personuppgifter eftersom de är svåra att förstå och få till antalet. IMY har inte följt upp vårdens och omsorgens behov av stöd eller utvärderat hur det befintliga stödet fungerar.

3.2.1 IMY:s stöd för skyddet av personuppgifter är generellt

Skydd av personuppgifter regleras i dataskyddsförordningen och kompletterande lagstiftning, och ska uppnås genom användning av lämpliga tekniska eller

[155] MSB:s föreskrifter om informationssäkerhet för statliga myndigheter framtagen med stöd av 21 § förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (MSBFS 2020:6). Den har ersatts av förordning (2022:524) om statliga myndigheters beredskap.

[156] Intervju med företrädare för MSB, 2023-05-11.

organisatoriska säkerhetsåtgärder i förhållande till risker som behandlingen medför.[157] IMY har en viktig roll i att vägleda[158] och stödja olika verksamheter, inklusive vård- och omsorgsgivare, för att tillämpa dataskyddsreglerna på ett korrekt sätt och för att skydda exempelvis känsliga personuppgifter.[159]

IMY:s stöd till vård- och omsorgsgivarnas arbete med att skydda personuppgifter enligt dataskyddsregelverket består av en generell vägledning om dataskyddsförordningen och hur den kan tillämpas. Den finns på IMY:s webbplats och är riktad till alla organisationer oavsett storlek eller verksamhetsområde. IMY hänvisar också till över 30 vägledningar från Europeiska dataskyddsstyrelsen (EDPB), varav flera berör dataskyddsfrågor.

IMY har också två specifika vägledningar för vården. En handlar om behovs- och riskanalys vid tilldelning av behörigheter[160] och en är checklista för logguppföljning av åtkomst till personuppgifter.[161] IMY anser att Socialstyrelsens föreskrifter innehåller tydliga krav på vissa säkerhetsåtgärder som är lämpliga enligt dataskyddsförordningen.[162] IMY ska också ge stöd genom att svara på frågor om hur dataskyddsreglerna kan tolkas, göra rättsliga ställningstagande och ge råd vid förhandssamråd och via sina tillsynsbeslut.

3.2.2 IMY:s generella stöd motsvarar inte vårdens och omsorgens behov

Våra intervjuer med sex kommuner och två regioner visar att IMY:s vägledningar inte i tillräcklig utsträckning stödjer deras informationssäkerhetsarbete. Det finns en rättslig osäkerhet hos regioner och framför allt hos kommuner om hur dataskyddsregelverket ska tolkas och tillämpas i det praktiska informationssäkerhetsarbetet i vården och omsorgen. Vård- och omsorgsgivare har behov av att få stöd i att tolka dataskyddsreglerna när de ska fatta beslut om vilka säkerhetsåtgärder som krävs för att uppfylla lagstiftningen. Flera kommuner och en region betonar att de, i brist på stöd, lägger betydande resurser på att tolka dataskyddsreglerna självständigt. Eftersom vård- och omsorgsgivare ibland gör olika tolkningar och beslut kan skyddet för personuppgifter variera över landet. Tydligare stöd i hur dataskyddsreglerna kan tolkas skulle enligt kommuner och regioner öka enhetligheten, underlätta för dem att fatta beslut om säkerhetsåtgärder och frigöra resurser för det faktiska informationssäkerhetsarbetet.[163]

157 Se artikel 32 dataskyddsförordningen.
158 Begreppet stöd förekommer inte i regleringen av IMY:s uppdrag. IMY använder begreppet vägledning som de menar är en form av stöd.
159 IMY:s svar på skriftliga frågor, 2023-10-04.
160 Datainspektionen 2020, *Behovs- och riskanalys inom hälso- och sjukvården – en vägledning*.
161 IMY, ”Systematisk logguppföljning”, hämtad 2023-10-26.
162 Intervju med företrädare för IMY, 2022-12-01 och intervju med företrädare för IMY, 2023-04-24.
163 Intervju med företrädare för kommun 2, kommun 3, kommun 6 och region 1.

Exempel på när det är svårt att fastställa lämpliga säkerhetsåtgärder för att upprätthålla adekvat informationssäkerhet är när:[164]

- servrar får placeras i Sverige eller utomlands,
- datalagring hanteras i amerikanska molntjänster,
- personuppgifter överförs till tredje land.

De efterfrågar också stöd för arbetet med att:[165]

- upphandla system som involverar informationssäkerhet, till exempel vid upphandling av digitala medicintekniska produkter,
- avgöra vilka riskområden och risker för informationssäkerhet som finns i vård- och omsorgssektorn,
- fastställa en lämplig miniminivå för säkerhetsåtgärder samt checklistor för praktisk tillämpning av informationssäkerhet,
- sammanställa befintlig rättspraxis inom området för att underlätta tolkningen av dessa frågor.

Två kommuner pekar på MSB:s metodstöd och pedagogiska material som ett bra exempel på hur IMY borde utforma sitt stöd.[166]

Regionerna anser att IMY inte ger dem tillräckligt med stöd för att hantera de komplexa avvägningarna som uppstår när man balanserar mellan olika lagar, särskilt när det gäller att förena informationssäkerhet och patientsäkerhet vid användning av digitala produkter inom vården.[167] En region efterfrågar stöd om vilken kryptering de ska använda för att skydda patienternas identitet vid sambearbetning av uppgifter. I brist på sådana föreskrifter[168] har regionen använt vägledning från andra länders motsvarighet till IMY.[169]

Företrädare för SKR påpekar att det är svårt för kommuner att fastställa lämpliga säkerhetsåtgärder när myndigheter inte specificerar en standard eller ger vägledning i vad som kan anses vara passande eller en lägstanivå. Detta kan leda till varierande tolkningar beroende på teknisk utveckling och den kunskapsnivå som finns i organisationerna. Det är framför allt mindre kommuner som saknar tillräckligt med kompetens och resurser.[170]

Samtliga sex kommuner och två regioner som vi har intervjuat har svårt att rekrytera och behålla kompetens inom informationssäkerhet. De två mindre kommunerna

164 Intervju med företrädare för kommun 3, kommun 4, kommun 5 och kommun 6.
165 Intervju med företrädare för kommun 1, kommun 3, kommun 4 och kommun 5.
166 Intervju med företrädare för kommun 3 och kommun 6.
167 Intervju med företrädare för region 1 och region 2.
168 IMY kan ge ut sådana föreskrifter enligt § 5 i patientdataförordningen.
169 Intervju med företrädare för region 1.
170 Intervju med företrädare för SKR, 2023-06-08.

betonar att de inte arbetar systematiskt med informationssäkerheten på grund av otillräckliga resurser och brist på kompetens samt att informationssäkerhetsarbetet inte är en prioriterad fråga i kommunen.[171]

Regeringen konstaterade 2020 att behovet av stöd och vägledning från IMY hade ökat påtagligt i både privat och offentlig sektor.[172] Regeringen har dock inte verkat för att IMY ska ta fram mer verksamhetsspecifik vägledning och stöd till bland annat vård- och omsorgsgivares arbete med att skydda personuppgifter. Enligt företrädare för Justitiedepartementet är IMY fullständigt oberoende i utförandet av sina uppgifter och regeringen är därför restriktiv i sin styrning av myndigheten.[173]

Brist på praxis och vägledning från EU försvårar konkret vägledning

IMY är medvetna om att det finns ett stort behov av vägledning i hur dataskyddsreglerna ska tolkas och tillämpas,[174] och att verksamheter vill få stöd i att navigera mellan en komplex lagstiftnings och en praktisk verklighet.[175] Enligt IMY skulle de kunna ge konkret och anpassad vägledning till vård- och omsorggivare genom att tolka regelverket och ta ställning i rättsliga frågor i betydligt större utsträckning än vad de gör idag. Men IMY har valt att ge generell vägledning som når ut till en bredare grupp verksamheter eftersom myndighetens ansvarsområde täcker alla sektorers personuppgiftsbehandling. Att ge sektorsspecifik vägledning om informationssäkerhet är enligt IMY inte möjligt.[176] IMY avvaktar resultatet av olika ärenden som är föremål för domstolsprövning, och vars utgång ännu inte har vunnit laga kraft, innan de överväger att uppdatera sin vägledning.[177]

Andra viktiga förklaringar till att IMY har svårt att ge konkret vägledning och tydligt stöd vid tolkning av regelverket är att det finns begränsad domstolspraxis från EU-domstolen och begränsad vägledning från EDPB på området.[178] IMY har därför som mål att ta tydlig ställning i rättsliga frågor och därigenom bidra till att utveckla praxis på nationell nivå.[179] Vår granskning visar dock att IMY sällan tar ställning i rättsliga frågor. Sedan 2018 har IMY endast publicerat fyra rättsliga ställningstaganden[180] där det saknas domstolspraxis eller vägledning. Inget av dessa rör vård eller omsorg.[181]

171 Intervju med företrädare för kommun 2 och kommun 5.
172 Prop. 2019/20:1 Utgiftsområde 1, s. 81.
173 Regeringskansliets svar på skriftliga frågor, 2023-10-03.
174 IMY, *Integritetsskyddsmyndighetens budgetunderlag 2022–2024*, 2021, s. 9 och IMY, *Integritetsskyddsmyndighetens budgetunderlag 2023–2025*, 2022, s. 5.
175 IMY, *Integritetsskyddsmyndighetens budgetunderlag 2024–2026*, 2023, s. 5.
176 IMY:s svar på skriftliga frågor, 2023-10-04. Se även e-post från IMY, 2024-02-14.
177 Intervju med företrädare för IMY, 2023-04-24.
178 Intervju med företrädare för IMY, 2023-03-30.
179 IMY, *IMY:s mål- och resultatkarta,* 2021.
180 IMYRS 2021:1, IMYRS 2022:1, IMYRS 2022:2 och IMYRS 2022:3.
181 Intervju med företrädare för IMY, 2022-12-01 och IMY:s svar på skriftliga frågor, 2023-10-04.

IMY ger sällan konkreta svar på hur bestämmelserna kan tolkas

För att få stöd i hur dataskyddsreglerna ska tolkas i förhållande till informationssäkerhet ställer vård- och omsorgsgivare regelbundet frågor till IMY.

Vår genomgång av inkomna kvalificerade frågor från vårdgivare och omsorgsgivare visar att IMY inte ger konkreta svar eller klargörande exempel på hur de kan hantera och skydda personuppgifter i sina verksamheter. I stället ger IMY generell vägledning och försöker hjälpa dem att förstå regelverket genom att hänvisa till relevanta artiklar i dataskyddsförordningen eller till information på deras webbplats. I en tredjedel av fallen hänvisar IMY till regionens eller kommunens dataskyddsombud för mer specifik vägledning.[182]

IMY betonar att frågorna ibland är beroende av sammanhanget och att IT-systemen inom vården och omsorgen är komplicerade. Därför undviker de att ge tydliga svar i specifika situationer, om inte Socialstyrelsens föreskrifter redan specificerat det, eftersom det kan leda till lösningar som inte är optimala. Andra viktiga förklaringar till att IMY inte ger konkret stöd är deras försiktighet med att tolka bestämmelserna. Enligt IMY skulle de behöva göra rättsliga ställningstaganden av bestämmelserna för att ge tydliga svar till verksamheter, vilket är svårt inom enskilda frågeställningar.[183] IMY betonar att de måste tolka dataskyddsförordningen tillsammans med andra dataskyddsmyndigheter för att säkerställa enhetlig tillämpning inom EU.[184] Enligt IMY gör dataskyddsmyndigheterna olika tolkningar av dataskyddsförordningen, och IMY behöver därför vara försiktiga i sin tolkning och samarbeta med andra dataskyddsmyndigheter för att få fram gemensam vägledning och praxis.[185] IMY anser att det även är en utmaning att balansera mellan att ge konkret stöd samtidigt som de bedriver tillsyn.[186]

Kommuner och regioner som vi har intervjuat har sökt stöd från IMY i olika informationssäkerhetsfrågor men anser att de i huvudsak inte fick det stöd som de behöver. Kommunerna berättar att de blev hänvisade till svårförståelig lagtext.[187] Ett exempel på behov av stöd är hur man prioriterar risker för personuppgifter i förhållande till bestämmelserna. En kommun tolkade att dataskyddsförordningen inte tillåter sannolikhetsbedömning av att en risk föreligger utan kräver att alla risker behandlas som höga. Enligt kommunen ställs de i en svår situation när de måste hantera potentiella risker utan möjlighet att bedöma om de verkligen utgör en hög

182 Se bilaga 2 för mer om inkomna frågor till IMY.

183 Intervju med företrädare för IMY, 2022-12-01, intervju med företrädare för IMY, 2023-04-24 och IMY:s svar på skriftliga frågor, 2023-10-04.

184 Tillämpningen av dataskyddsförordningen ställer krav på harmonisering, vilket innebär att alla dataskyddsmyndigheter ska tolka och tillämpa dataskyddsförordningen på samma sätt så att tillämpningen blir enhetlig över hela unionen.

185 Intervju med företrädare för IMY, 2022-12-01, intervju med företrädare för IMY, 2023-04-24 och IMY:s svar på skriftliga frågor, 2023-10-04.

186 Intervju med företrädare för IMY, 2022-12-01.

187 Intervju med företrädare för kommun 1, kommun 2, kommun 3, kommun 4 och kommun 6.

risk i jämförelse med andra bestämmelser och behov inom vården och omsorgen. Kommunen hade behövt vägledning om risker och riskbedömningar.[188]

De två intervjuade regionerna anser att IMY inte gav dem tillräckligt med stöd för att hantera komplexa avvägningar mellan olika bestämmelser.[189] En region betonar att IMY inte förstår deras verksamhet och sådana målkonflikter. Till exempel har regionen frågat IMY om anonymisering och pseudonymisering men fått ett vagt svar, med huvudbudskapet att anonymisering inte är genomförbart.[190]

Vägledningsarbetet på EU-nivå tar lång tid och omfattar kompromisser

IMY lägger mycket tid och resurser på samarbete med andra dataskyddsmyndigheter inom EDPB[191] för att ta fram gemensamma vägledningar.[192] IMY anser att det finns utmaningar i samarbetet, särskilt när det gäller tolkningen av dataskyddsförordningen, vilket kan leda till kompromisser i vägledningar och göra dem mindre konkreta och tydliga. Strävan efter konsensus inom EDPB kan förlänga processen med att ta fram en vägledning och göra den föråldrad på grund av snabb teknisk utveckling och förändringar i domstolspraxis.[193]

IMY deltar aktivt i de flesta arbetsgrupper för vägledningar inom EDPB och leder arbetet med flera vägledningar. Under 2022 deltog IMY i drygt hundra arbetsgruppsmöten.[194] IMY anser att dataskyddsförordningen har förändrat samarbetet mellan EU:s dataskyddsmyndigheter i grunden och anser sig stå på två ben, dels som en nationell tillsynsmyndighet, dels som en del av EDPB där huvuddelen av utvecklingen och tolkningen av lagstiftningen sker.[195]

Processtöd för vägledningsarbetet på plats först 2024

Fram till 2023 hade IMY ingen strukturerad arbetsprocess för att skapa vägledning och stöd till olika verksamheter.[196] Redan 2022[197] insåg IMY behovet av att förbättra sitt arbete med att ta fram vägledningar för olika verksamheter. Beslutet att förbättra arbetet med vägledning vad gäller dataskyddsförordningen togs i september 2023. Under 2024 är en av IMY:s huvudprioriteringar att intensifiera och bredda arbetet med vägledning för olika teman baserat på identifierade behov från olika sektorer. En prioriterad vägledningsaktivitet är konsekvensbedömningar, vilket var något som IMY identifierade som ett område som fler aktörer vill ha vägledning i. IMY har inte

188 Intervju med företrädare för kommun 3.
189 Intervju med företrädare för region 1 och region 2.
190 Intervju med företrädare för region 2.
191 Inom EDPB finns dataskyddschefer från EU länders myndigheter med starka mandat att fatta beslut och ge ut gemensamma vägledningar för hur man ska tolka och tillämpa regelverket.
192 IMY:s svar på skriftliga frågor, 2023-10-04.
193 Intervju med företrädare för IMY, 2022-12-01, intervju med företrädare för IMY, 2023-04-24 och IMY:s svar på skriftliga frågor, 2023-10-04.
194 IMY, *Årsredovisning 2022*, 2023, s. 27–29.
195 IMY, *Årsredovisning 2020*, 2021, s. 40.
196 Intervju med företrädare för IMY, 2023-04-24.
197 Se IMY:s verksamhetsplan för 2023 (IMY-2022-158).

beslutat om kommande vägledningar ska rikta sig specifikt till vård- och omsorgssektorn.[198]

3.2.3 Förhandssamråd används sällan för att ge konkret stöd

Personuppgiftsansvariga måste, enligt dataskyddsförordningen, begära ett förhandssamråd med IMY innan de påbörjar personuppgiftsbehandling som medför hög risk för enskildas fri- och rättigheter. Denna begäran föregås av en konsekvensbedömning som visar på en kvarstående hög risk[199] för personers rättigheter och friheter, inklusive skyddet av personuppgifter. IMY ska ge råd om hur man kan hantera riskerna eller förbjuda behandlingen om den inte är förenlig med dataskyddsförordningen.[200] Förhandssamrådet kan därmed fungera som ett konkret stöd när det gäller informationssäkerhet. Vår granskning visar dock att IMY inte har gett tillräckligt med stöd till vård- och omsorgsgivare via förhandssamråd.

Mellan 2018 och 2023 ansökte organisationer om 85 förhandssamråd hos IMY, varav 6 var från vård- och omsorgsgivare.[201] Samtliga 6 avvisades eftersom de inte uppfyllde kraven, till exempel på grund av otillräckliga underlag eller för att personuppgiftsbehandlingen redan hade påbörjats. IMY anser att alltför få förfrågningar om förhandssamråd kommer in till myndigheten, vilket hindrar IMY från att ge råd eller vidta åtgärder för att minska riskerna för skyddet av personuppgifter.[202] IMY anser att det inte behöver införas krav[203] på förhandstillstånd för vissa personuppgiftsbehandlingar som fallet var enligt tidigare lagstiftning. Enligt IMY kan de ge vägledning till verksamheterna i samma frågor utanför förhandssamrådet om verksamheterna söker stöd från myndigheten.[204]

IMY upplever att organisationer inte begär förhandssamråd eftersom de felaktigt bedömer riskerna i sina konsekvensbedömningar eller att de inte är medvetna om kraven. Två kommuner och en intervjuad region anser att organisationer inte begär förhandssamråd eftersom IMY oftast avslår ansökningarna utan att ge alternativa lösningar på hur de skulle kunna minska riskerna. Exempel på sådana situationer är de behandlingar som inleddes före dataskyddsförordningen vilka är ett hinder för att begära förhandssamråd och få råd.[205] En kommun hade sökt vägledning från IMY i samma frågor utanför förhandssamrådet men inte fått det.[206] Ett fall som IMY avvisade överklagades till förvaltningsrätten som dock upphävde IMY:s

198 IMY:s svar på skriftliga frågor, 2023-10-04 och e-post från IMY, 2023-11-23.
199 En risk kan vara teknisk på så sätt att man inte kan få till en proportionerlig skydd.
200 Intervju med företrädare för IMY, 2022-12-01.
201 Tre enskilda vårdgivare, två vårdgivare från regioner och en omsorgsgivare hade inkommit med förhandssamråd till IMY mellan 2018 och oktober 2023. Se e-post från IMY, 2023-03-16.
202 IMY:s svar på skriftliga frågor, 2023-10-04 och intervju med företrädare för IMY, 2023-03-08.
203 Artikel 36.5 i dataskyddsförordningen anger att det finns utrymme för den svenska lagstiftaren att införa nationella lagar och förordningar som reglerar att en personuppgiftsansvarig måste ha förhandstillstånd för vissa typer av personuppgiftsbehandling.
204 IMY:s svar på skriftliga frågor, 2023-10-04.
205 Intervju med företrädare för kommun 2, kommun 3 och region 2.
206 Intervju med företrädare för kommun 3.

avvisningsbeslut. Domstolen fann att enbart den omständigheten att behandlingarna har påbörjats inte utgör skäl att avvisa sökandens begäran varför ärendet återförvisades för ny handläggning hos IMY.[207]

SKR anser att förhandssamråd kommer sent i processen och att det krävs hög kompetens inom organisationer för att bedöma konsekvenserna. Enligt SKR bör IMY vara mer proaktiv och ge stöd tidigare.[208]

IMY försöker öka kunskapen om konsekvensbedömningar genom vägledande information på sin webbplats, seminarier och utbildningar. IMY planerar att utveckla vägledningen om konsekvensbedömningar under 2024 för att öka förståelsen för reglerna.[209]

3.2.4 Svårt att använda tillsynsbesluten som vägledning

IMY anser att deras tillsynsbeslut inom vården kan fungera som vägledning för liknande verksamheter eftersom de tydliggör lämpliga åtgärder för bland annat skydd av personuppgifter.[210]

Dock anser flera intervjuade kommuner och regioner att tillsynsbesluten är svåra att använda som vägledning för skydd av personuppgifter. En kommun anser att beslutens motivering är svåra att förstå på grund av det juridiska språket.[211] En annan kommun betonar att det finns för få beslut inom vården som är vägledande.[212]

Ett dataskyddsombud anser att tillsynsbesluten är öppna för olika tolkningar, vilket skapar förvirring bland verksamheterna när de ska omsätta besluten i praktiken.[213] En region anser att tillsynsbesluten bara täcker en del av behoven av vägledning för vården och efterfrågar mer förebyggande stöd.[214]

IMY har förståelse för att besluten är juridiskt komplicerade och svåra att förstå.[215] För att göra tillsynsbesluten mer praktiskt användbara för vårdgivarna utvecklade dåvarande Datainspektionen 2020 en vägledning för behovs- och riskanalys vid behörighetstilldelning[216] i samband med tillsyn av åtta vårdgivare.

---

207 Dom av Förvaltningsrätten i Stockholm som avsåg en kommunal nämnd i Göteborgs stad, mål nummer 4721-22, meddelad 16 november 2023. IMY har valt att inte överklaga domen. IMY har påpekat att Göteborgs stad har återkallat sin begäran om förhandssamråd.

208 Intervju med företrädare för SKR, 2023-06-08.

209 IMY:s svar på skriftliga frågor, 2023-10-04 och intervju med företrädare för IMY, 2023-03-08.

210 Intervju med företrädare för IMY, 2023-04-24.

211 Intervju med företrädare för kommun 1.

212 Intervju med företrädare för kommun 3.

213 Intervju med företrädare för kommun 6.

214 Intervju med företrädare för region 1.

215 Intervju med företrädare för IMY, 2022-12-01.

216 Datainspektionen, *Behovs- och riskanalys inom hälso- och sjukvården – en vägledning*, 2020.

3.2.5 Få utbildningar som delvis berör informationssäkerhet

IMY framhåller att utbildning är en viktig kanal för att ge vägledning och stöd. Fram tills 2020 höll IMY i en 1–2 dagars utbildning om säkerhetsbestämmelser i dataskyddsförordningen för alla sektorer. Från och med 2020 övergick de till en timmes årlig digital grundutbildning för att utöka tillgängligheten.[217]

Våra intervjuer med kommuner visar att de vill ha mer fördjupade och praktiskt anpassade utbildningar. En kommun betonar att IMY:s utbildning i dataskyddsförordningen inte är tillräckligt praktisk för att stödja arbetet med säkerhetsåtgärder i verksamheten.[218] Kommunerna efterfrågar konkreta utbildningar om exempelvis riskanalyser och de specifika risker som är relevanta inom vården och omsorgen samt utbildningar för roller såsom informationssäkerhetssamordnare.[219] En annan kommun lyfter MSB:s utbildningar för informationssäkerhet som goda exempel som bidrar till att stärka medarbetarnas kompetens. Kommunen upplever att IMY saknar motsvarande utbildningar för dataskydd.[220]

IMY deltar i ”Tänk säkert”-kampanjen[221] som syftar till att öka medvetenheten om informations- och cybersäkerhetsfrågor och håller webbinarier om ämnen såsom personuppgiftsincidenter och säkerhetsåtgärder. IMY håller också föreläsningar och har till exempel deltagit i SKR:s nätverk för socialtjänsten. IMY har dessutom årligen en digital konferens för dataskyddsombud från alla sektorer.[222]

3.2.6 De flesta personuppgiftsincidenter avslutas utan åtgärder och hanteras inte effektivt

Alla organisationer ska inom 72 timmar rapportera personuppgiftsincidenter[223] till IMY genom ett formulär på deras webbplats. Innan personuppgiftsansvariga anmäler en incident ska de bedöma om det är troligt att incidenten innebär en risk för de berörda individernas fri- och rättigheter.[224] IMY har tagit fram flera exempel på webbplatsen som kan vara vägledande i riskbedömningen. EDPB har också en vägledning för hur olika typer av incidenter bör hanteras.[225]

IMY utreder inte alla incidenter utan väljer manuellt ut de som anses ha högst risk utifrån vissa kriterier.[226] De allra flesta incidenterna avslutas utan åtgärder och utan

---

217 Intervju med företrädare för IMY, 2022-12-01 och IMY:s svar på skriftliga frågor, 2023-10-04.

218 Intervju med företrädare för kommun 6.

219 Intervju med företrädare för kommun 1 och kommun 2.

220 Intervju med företrädare för kommun 3.

221 MSB och Polismyndigheten ansvarar för kampanjen.

222 Intervju med företrädare för IMY, 2022-12-01 och IMY:s svar på skriftliga frågor, 2023-10-04.

223 En personuppgiftsincident är en säkerhetsincident som innebär att personuppgifter har blivit förstörda, förlorade, ändrade eller att obehöriga har haft tillgång till dem (informationssäkerhet). Se artikel 4.12 i dataskyddsförordningen.

224 Artikel 33, dataskyddsförordning och 2 a § förordningen med instruktion för Integritetsskyddsmyndigheten.

225 EDPB, *Riktlinjer 01/2021 om exempel på anmälan av personuppgiftsincidenter,* 2021.

226 Kriterierna omfattar bland annat orsaker och allvarlighetsgrad. Exempel på orsaker är antagonistiskt angrepp och exempel på allvarlighetsgrad är känslighetsgraden och omfattningen av personuppgifterna.

att IMY utvärderar hur organisationen hanterade dem. I de få fall där det bedöms att det finns en hög risk överlämnas incidenterna till operativa tillsynsenheter som bedömer om tillsyn ska inledas eller inte.[227]

Flera intervjuade kommuner och en region anser att anmälningsprocessen för incidenter behöver förbättras och förenklas. De är osäkra på vilka incidenter som ska rapporteras[228] och föreslår att det borde finnas en enda kanal för att rapportera olika incidenter till alla berörda myndigheter.[229] De anser också att IMY:s anmälningsformulär är komplicerat och bör förenklas.

En kommun föreslår att IMY kompletterar formulären med informationstexter för att göra frågorna tydligare. De vill också ha tydliga kriterier för att bedöma allvarliga och mycket allvarliga incidenter. Kommunen vill även att IMY tydligt förklarar i besluten varför de inte utreder incidenter. Det skulle ge dem vägledning för framtida åtgärder vid liknande incidenter. Kommunen anser att bristen på återkoppling, och det faktum att incidenter sällan leder till tillsyn, inte uppmuntrar verksamheterna att anmäla incidenter till IMY.[230]

En annan kommun anser att IMY bör inleda mer tillsyn baserat på incidenter. Eftersom IMY oftast bara avslutar incidentärenden utan åtgärder kan det leda till att riskerna kvarstår i verksamheterna.[231] En annan kommun anser att Socialstyrelsen borde analysera incidenterna och vilka konsekvenser som de medför, och vägleda i hur ska man hantera det inom vården och omsorgen.[232]

Personuppgiftsansvariga som har anmält incidenter har behövt vänta länge på besked om att ärendet avslutats. Under 2022 avslutades 67 procent av alla incidenter inom 30 dagar.[233] Långa handläggningstider beror enligt IMY på att vissa anmälningar saknar nödvändig information och behöver kompletteras. En annan orsak är att hanteringen av incidenterna inte är digitaliserad och måste utföras manuellt, vilket är resurskrävande. En tredje orsak är IMY:s prioritering av arbetet med klagomål, vilket har minskat resurserna till hanteringen av personuppgiftsincidenter.[234]

IMY analyserar inte orsaker till mörkertalet

IMY bedömer att det finns ett stort mörkertal av anmälningspliktiga personuppgiftsincidenter[235] som inte rapporteras till myndigheten. De är medvetna om att vissa sektorer och verksamheter inte rapporterar incidenter. Men IMY har inte undersökt varför alla incidenter inte rapporteras och i vilka sektorer som problemet är

227 Intervju med företrädare för IMY, 2023-05-02.
228 Intervju med företrädare för kommun 2 och kommun 3.
229 Intervju med företrädare för kommun 2 och region 1.
230 Intervju med företrädare för kommun 3.
231 Intervju med företrädare för kommun 6.
232 Intervju med företrädare för kommun 1.
233 IMY, *Årsredovisning 2022*, 2023, s. 29–30, 33.
234 Intervju med företrädare för IMY, 2023-05-02.
235 Det betyder att antalet incidenter som faktiskt inträffar varje år är större än vad som redovisas.

störst. IMY har inte heller undersökt vilka vårdgivare och omsorgsgivare inom regioner och kommuner som rapporterar och vilka som inte gör det.[236] Därför är det oklart om de incidentanmälningar som IMY har fått ger en korrekt bild av problemen i vårdens och omsorgens informationssäkerhet. Sammantaget innebär mörkertalet och bristen på analyser att risken är att IMY inte inriktar tillsynen mot de mest relevanta problemområdena och inte förbättrar stödet som behövs för att höja nivån på informationssäkerheten inom olika verksamheter.

Företrädare för IMY betonar att mörkertalet är svårt att mäta men att de skulle kunna minska underrapporteringen inom vården genom att granska vårdgivare som inte har anmält incidenter och jämföra deras dataskyddsarbete[237] med de vårdgivare som har anmält incidenter.[238]

Enligt IMY kan det vara svårt för vård- och omsorgsgivare att veta till vilken myndighet de ska anmäla en incident. För att fler verksamheter ska anmäla incidenter, både om personuppgifter till IMY och om IT-incidenter till MSB, anser IMY att det behövs en enklare kanal via en webbplats för att rapportera incidenter och att berörda myndigheter behöver samarbeta i detta. IMY samverkar dock inte med MSB eller Polismyndigheten om inrapporterade incidenter. Enligt IMY behöver de också samverka med Socialstyrelsen och dela analyser av personuppgiftsincidenter från vården och omsorgen så att Socialstyrelsen kan förbättra sitt stöd. IMY tror också att sekretess för incidentanmälningarna skulle minska mörkertalet. IMY påtalar skyldigheten att anmäla incidenter på sin webbplats men har inte verkat för att främja rapporteringsviljan genom riktad information till vård- och omsorgsgivare.[239]

Det pågår ett utvecklingsarbete med personuppgiftsincidenterna

IMY identifierade 2022 behovet av att effektivisera processen för hantering av incidenter. Beslutet att utvecklingsarbetet ska bedrivas i projektform togs i april 2023. IMY såg också behov av tydligare rutiner och stöd för personalen i handläggningen av incidenter. Målet är att implementera ett digitalt ärendehanteringssystem som kan automatisera hanteringen av anmälda incidenter och effektivisera det riskbaserade urvalet av incidenterna. Detta system förväntas bli upphandlat under 2024.[240]

För att det nya ärendesystemet ska fungera väl är det avgörande att informationen i incidentanmälningarna är korrekt och fullständig. IMY arbetar med att förbättra vägledningen så att verksamheterna kan fylla i formuläret korrekt.[241]

---

236 Intervju med företrädare för IMY, 2022-12-01 och intervju med företrädare för IMY, 2023-03-30. Se även IMY, *Anmälda personuppgiftsincidenter 2021,* 2022, s. 27 och IMY, *Anmälda personuppgiftsincidenter 2022,* 2023, s. 30, 47.

237 Systematiskt dataskydd är att arbeta förebyggande och kontinuerligt i verksamheten för att skydda personuppgifter som verksamheten behandlar (informationssäkerhet).

238 Intervju med företrädare för IMY, 2022-12-01 och intervju med företrädare för IMY, 2023-03-30.

239 Intervju med företrädare för IMY, 2023-05-02.

240 IMY, *Projektdirektiv – Utveckla arbetet med anmälda personuppgiftsincidenter,* 2023.

241 Intervju med företrädare för IMY, 2023-05-02.

3.2.7 IMY följer inte upp vårdens och omsorgens behov av stöd

IMY har inte undersökt vilket stöd olika verksamheter, inklusive vården och omsorgen, behöver när det gäller informationssäkerhet för personuppgifter. IMY har inte heller utvärderat hur deras befintliga vägledning och stöd för informationssäkerhet fungerar för vård- och omsorgsgivare. Anledningen till det är enligt IMY att en sådan utvärdering kan liknas vid en tillsyn där det bedöms om vårdgivare och omsorgsgivare drar nytta av att följa regelverket. I stället anser IMY att de kan förstå behoven och förbättra sin vägledning genom dialog med externa aktörer.[242] Statskontoret rekommenderade IMY 2020 att följa upp om effekterna av myndighetens stöd- och vägledningsinsatser svarar mot olika målgruppers behov.[243]

3.3 Socialstyrelsen brister i sin styrning av vårdens informationssäkerhet och ger inte specifikt stöd

Socialstyrelsen har meddelat föreskrifter och allmänna råd om journalföring och personuppgiftsbehandling vilka kompletterar PDL. Föreskrifterna gäller inte för omsorgsverksamhet inom socialtjänsten. Socialstyrelsen har inte meddelat föreskrifter till NIS-lagen vilket har begränsat IVO:s möjligheter att bedriva tillsyn av säkerheten i vårdgivarnas nätverk och informationssystem. Socialstyrelsen har tagit fram en handbok till stöd för vårdgivarnas tillämpning av föreskrifterna kring journalföring och personuppgiftsbehandling, men den bidrar i begränsad omfattning till informationssäkerhetsarbetet. Socialstyrelsen ger inte specifikt stöd till vård- och omsorgsgivares informationssäkerhetsarbete eftersom de inte anser att det ingår i deras uppdrag. Myndigheten saknar också kompetens inom informationssäkerhet.

3.3.1 Socialstyrelsens föreskrifter omfattar enbart vården

För att komplettera och precisera kraven i PDL har Socialstyrelsen meddelat föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i vården.[244] Föreskrifterna gäller endast för vården och innehåller bestämmelser för hantering och skydd av personuppgifter.[245] Socialstyrelsen har tagit fram en handbok som stöd till vårdgivare vid tillämpningen av föreskrifterna.[246] Socialstyrelsen tillhandahåller också ett webbaserat stöd som beskriver regelverket för informationshantering utifrån gällande rätt.

Omsorgsverksamheter inom socialtjänsten hanterar liknande känsliga personuppgifter som vården. Dessa uppgifter regleras i lagen (2001:454) om

---

242 Intervju med företrädare för IMY, 2023-04-24.

243 Statskontoret, *Myndighetsanalys av Datainspektionen*, 2020, s. 91.

244 Socialstyrelsen, (*HSLF-FS 2016:40) Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården,* 2016.

245 I 3 kap. 2 § i föreskriften ställs krav på att vårdgivare ska ha ett ledningssystem för systematiskt kvalitetsarbete som ska innehålla de processer och rutiner som krävs för att säkerställa kraven på informationssäkerhet (tillgänglighet, riktighet, konfidentialitet och spårbarhet). Det finns dock inga krav på att ledningssystemet ska bygga på standarder i ISO/IEC 27000-serien.

246 Socialstyrelsen, *Journalföring och behandling av personuppgifter i hälso- och sjukvården*, 2017.

behandling av personuppgifter inom socialtjänsten. Fram till den 1 mars 2024 berörde inte lagen informationssäkerhet, vilket innebar att kravet på att skydda personuppgifter inte var lika tydligt för omsorgsgivare som för vårdgivare.[247]

3.3.2 Stödet för tillämpning av bestämmelserna är otillräckligt

Våra intervjuer med två regioner och sex kommuner visar att Socialstyrelsens stöd när det gäller informationssäkerhetsarbetet är otillräckligt för deras behov. Trots föreskrifterna om journalföring och behandling av personuppgifter och handboken saknar de stöd med konkreta exempel på hur de ska tillämpa bestämmelserna praktiskt. Regioner och kommuner efterfrågar stöd som är anpassat efter vård- och omsorgsverksamheter och behöver stöd för att tolka bestämmelserna, särskilt i situationer som kräver svåra uttolkningar av regelverket vid avvägningar mellan informationssäkerhet, integritet och patientsäkerhet.

En av regionerna anser att föreskrifterna och handboken är föråldrade och inte följer utvecklingen efter att dataskyddsförordningen och NIS-lagen trädde i kraft. Som ett exempel på svår avvägning nämner regionen att PDL och Socialstyrelsens föreskrifter ställer specifika krav på åtkomst av patienters identitet, men att leverantörer av medicinteknisk utrustning inte kan leverera produkter med tillräckligt stark autentisering.[248] En annan region anser att Socialstyrelsen skulle kunna ge mer konkret vägledning, till exempel om vilka större risker som finns inom vården och omsorgen och hur de kan förhålla sig till riskerna.[249] (Se avsnitt 3.2.2 för mer om vård- och omsorgsgivarnas behov av stöd.)

Företrädare för MSB anser att Socialstyrelsens föreskrifter inte är tillräckligt utförliga och omfattar journalsystem men inte andra IT-system inom vården.[250]

Socialstyrelsen har inte uppdaterat föreskrifterna eller handboken sedan 2016.[251] Socialstyrelsen menar att det är ett resurskrävande arbete att revidera föreskrifterna. De behöver först samla och sammanställa alla synpunkter som de fått in och skapa sig en bild av vad som ska förändras, och sedan behöver flera remissrundor göras innan en förändring kan göras. Socialstyrelsen har fått flera synpunkter, till exempel att loggar och signeringskravet behöver ses över.[252]

---

247 Från och med 1 mars 2024 infördes nya bestämmelser som innebär krav på behörighetstilldelning och kontroll av åtkomst, se 10 § lagen om behandling av personuppgifter inom socialtjänsten, prop. 2022/23:131, bet. 2023/24:SoU3, rskr. 2023/24:46.

248 Intervju med företrädare för region 1.

249 Intervju med företrädare för region 2.

250 Intervju med företrädare för MSB, 2022-12-16.

251 Formella ändringar har gjorts i föreskriften föranlett av ändringar i anslutande reglering och dataskyddsförordningens ikraftträdande.

252 Intervju med företrädare för rättsavdelningen på Socialstyrelsen, 2022-11-24.

3.3.3 Socialstyrelsen ger inte stöd vid tolkning av bestämmelserna

Socialstyrelsen ger inte vård- och omsorgsgivare stöd vid tolkning av bestämmelserna om hur de kan skydda personuppgifter i praktiken. Socialstyrelsen återger oftast bara vad som står i PDL eller föreskrifterna. En viktig förklaring till det är att Socialstyrelsen inte tolkar lagstiftningen som berör informationssäkerhet, varken generellt eller i enskilda fall. Det innebär att myndigheten inte ger konkret stöd om vilka säkerhetsåtgärder som är lämpliga för att skydda personuppgifter.[253] En annan orsak är att Socialstyrelsen saknar kompetens inom informationssäkerhet. Företrädare för myndighetens rättsavdelning uppger att de är medvetna om att detta begränsar Socialstyrelsens stödjande insatser. Ett viktigt skäl till att myndigheten inte ger konkret stöd om hur bestämmelserna kan tillämpas i enskilda fall är att det ofta saknas rättspraxis och att rättsläget är oklart. Socialstyrelsen anser därför att det finns en risk med att tolka lagstiftningen och är försiktig med att ge konkret stöd i enskilda fall när rättsläget är oklart eftersom en tillsynsmyndighet eller en domstol kan göra en annan bedömning. Socialstyrelsen anser att eventuellt konkret stöd från dem kan komma att ifrågasättas senare av andra aktörer, vilket enligt myndigheten kan leda till ökade kostnader för vård- och omsorgsgivare och eventuellt leda till skadeståndskrav mot Socialstyrelsen.[254]

Ingen av de sex intervjuade kommunerna och de två regionerna har sökt stöd från Socialstyrelsen eftersom de uppfattar att myndigheten inte ger stöd vid tolkning av regelverken. SKR betonar att de upplever att Socialstyrelsen inte har en tydlig roll i att ge stöd till vården och omsorgen rörande informationssäkerhet.[255]

Företrädare för rättsavdelningen anser att Socialstyrelsen inte har ett tydligt uppdrag att ge stöd till vårdens och omsorgens informationssäkerhetsarbete eftersom informationssäkerhet inte nämns i myndighetens instruktion. De anser att IMY har kompetens inom informationssäkerhet och är den myndighet som ska ge stöd i sådana frågor. När det gäller NIS-lagen anser Socialstyrelsen att de har ett snävt uppdrag och enbart ska normera via föreskrifter till lagen.[256]

3.3.4 Socialstyrelsen har inte tagit fram föreskrifter till NIS-lagen vilket har begränsat vägledning och tillsynen

Socialstyrelsen har inte utfärdat föreskrifter om säkerhetsåtgärder för vårdsektorn enligt den så kallade NIS-lagen som trädde i kraft 2018. Det innebär att vården inte har fått vägledning om vad som krävs för att de ska uppfylla kraven på säkerhetsåtgärder för informationssäkerhet i informationssystem där känsliga personuppgifter behandlas. Det har också begränsat IVO:s tillsyn av säkerheten i vårdens nätverk och informationssystem (se avsnitt 4.2.1).

253 Intervju med företrädare för Socialstyrelsen, 2023-04-13 och 2022-11-24.
254 Intervju med företrädare för Socialstyrelsen, 2022-11-24 och e-post från Socialstyrelsen, 2024-02-12.
255 Intervju med företrädare för SKR, 2023-06-08.
256 Intervju med företrädare för Socialstyrelsen, 2022-11-24.

Företrädare för SKR betonar att kommuner och regioner vill ha tydlig vägledning om vad som förväntas av dem för att de ska kunna leva upp till NIS-lagen.[257] De två intervjuade regionerna anser att de behöver föreskrifter till NIS-lagen när de ska vidta säkerhetsåtgärder för att skydda informationen.[258]

Syftet med NIS-lagen är att uppnå hög nivå på säkerheten i nätverk och informationssystem. Regeringen har i Socialstyrelsens regleringsbrev för 2019 och 2020 ställt rapporteringskrav på myndigheten att redovisa arbetet med föreskrifter till NIS-lagen.[259] Socialstyrelsen bedömer att beslut om föreskrifter kommer att fattas först under våren 2024.[260] Socialdepartementet har inte följt upp varför Socialstyrelsen inte har tagit fram föreskrifter.[261] Andra sektorsmyndigheter, såsom Post- och telestyrelsen, Energimyndigheten och Transportstyrelsen, meddelade föreskrifter och allmänna råd till NIS-lagen under 2021 och 2022.

Socialstyrelsen saknar kompetens och dröjde med att söka stöd

Enligt Socialstyrelsen är brist på kompetens samt pandemin viktiga orsaker till att arbetet med föreskrifter till NIS-lagen dröjer. När NIS-lagen trädde i kraft saknade Socialstyrelsen den kompetens inom informationssäkerhet och av vårdens informationstekniska behov som behövs för att kunna ta fram föreskrifterna. Under 2020 och 2021 prioriterade rättsavdelningen arbetet med covid-19 pandemin.[262]

För att skaffa nödvändig kompetens försökte Socialstyrelsen upphandla en konsult i oktober 2020 men fick inga anbud trots flera försök, troligen på grund av den låga omfattningen av uppdraget. Socialstyrelsen sökte därefter stöd från IVO som erbjöd sig att bistå med kompetens. IVO och Socialstyrelsen hade åtta möten under 2021 och 2022 om arbetet med föreskrifterna. IVO lämnade i september 2023 synpunkter på Socialstyrelsens utkast till föreskrifter.[263]

Socialstyrelsen har inte involverat vårdgivare i arbetet med att ta fram föreskrifterna till NIS-lagen, vilket har begränsat deras möjlighet att bidra med sina perspektiv.

Socialstyrelsen har inte samarbetat med MSB för att ta fram föreskrifterna eftersom de ansåg att MSB saknade den kompetens som behövdes.[264] MSB har varit sammankallande till ett samarbetsforum för NIS-lagen där arbetet med föreskrifterna har diskuterats men Socialstyrelsen deltog endast i början.[265] Enligt Socialstyrelsen slutade de att delta eftersom fokus skiftade från föreskriftsarbete till tillsyn.[266]

---

257 Intervju med företrädare för SKR, 2023-06-08.
258 Intervju med företrädare för region 1 och region 2.
259 Regeringsbeslut S2019/04518/FS och regeringsbeslut S2020/09552.
260 Socialstyrelsens svar på skriftliga frågor, 2023-09-22.
261 Regeringskansliet svar på skriftliga frågor, 2023-10-03.
262 Intervju med företrädare för rättsavdelningen på Socialstyrelsen, 2022-11-24. Se även Socialstyrelsen, *Årsredovisning 2019*, 2020, s. 74 och Socialstyrelsen, *Årsredovisning 2020*, 2021, s. 115.
263 Intervju med företrädare för rättsavdelningen på Socialstyrelsen, 2022-11-24 och e-post från Socialstyrelsen, 2023-05-02.
264 Socialstyrelsens svar på skriftliga frågor, 2023-09-22.
265 Intervju med företrädare för IVO, 2023-04-19 och intervju med företrädare för MSB, 2022-12-16.
266 E-post från Socialstyrelsen, 2024-02-12.

Socialstyrelsen använder inte IT-incidentrapportering från vården

Socialstyrelsen får vårdens IT-incidentrapporter från MSB men använder inte dem i arbetet med föreskrifter till NIS-lagen eller för att förbättra stödet. Detta trots att incidentrapporterna kan vara ett underlag när nya föreskrifter avseende tekniska och organisatoriska åtgärder ska tas fram[267] och ett underlag för att utveckla.[268] Men företrädare för Socialstyrelsens rättsavdelning anser att det inte är användbart att analysera dessa incidentrapporter. Avdelningen för krisberedskapen var fram tills 2022 mottagare av incidentrapporterna men har inte heller använt dem i sitt arbete.[269]

3.3.5 Få kommuner använder statsbidrag som bland annat kan användas för att stärka informationssäkerheten

På uppdrag av regeringen fördelade Socialstyrelsen varje år mellan 2021 och 2023 knappt 4 miljarder kronor till kommuner för att säkerställa god vård och omsorg av äldre personer. Medlen fick användas utifrån lokala behov i syfte att förbättra och utveckla hela verksamheten, däribland informationssäkerheten.[270]

Socialstyrelsens uppföljning av statsbidragets användning under 2021 och 2022 visar att 30 respektive 35 av 290 kommuner har använt statsbidraget för att stärka informationssäkerheten för olika digitala lösningar. Dessa kommuner har dessutom i mycket låg utsträckning använt statsbidraget för att stärka informationssäkerheten.[271] Åtgärderna som vidtagits med hjälp av statsbidragen har framför allt handlat om att införa Klassa-verktyget från SKR, säkerställa behörig åtkomst till digitala läkemedelsskåp, införa tvåfaktorsinloggning och genomföra informationssäkerhetsutbildningar.[272]

3.3.6 Socialstyrelsen följer upp kommunernas informationssäkerhetsarbete …

Socialstyrelsen har i årliga uppföljningar av kommunernas informationssäkerhetsarbete identifierat flera brister (se avsnitt 2.4)[273] men har inte använt informationen systematiskt för att utforma stödjande insatser till kommunernas informationssäkerhetsarbete. Socialstyrelsen sammanställer resultaten i årliga rapporter och i ett webbverktyg där kommunerna kan ta del av sitt resultat och jämföra sitt resultat med andras. Socialstyrelsen ger inte individuell återkoppling till enskilda kommuner på grund av resursbrist. Enligt Socialstyrelsen är

267 SOU 2017:36. Se även Regeringskansliets svar på skriftliga frågor, 2023-10-03.
268 Intervju med företrädare för MSB, 2022-12-12.
269 Intervju med företrädare för beredskapsenheten på Socialstyrelsen, 2022-12-05.
270 Regeringsbeslut S2021/07588 (delvis), S2022/04549 och S2023/02343.
271 Intervju med företrädare för Socialstyrelsen, 2023-04-14. Se även Socialstyrelsen, *Redovisning av 2022 års statsbidrag till kommuner för att säkerställa god vård och omsorg av äldre personer*, 2023, s. 11.
272 Socialstyrelsen, *Redovisning av 2022 års statsbidrag till kommuner för att säkerställa god vård och omsorg av äldre personer*, 2023, s. 8, 11 och Socialstyrelsen, *Redovisning av 2021 års statsbidrag till kommuner för att säkerställa god vård och omsorg av äldre personer*, 2022, s. 8. Se även e-post från Socialstyrelsen, 2023-04-14.
273 Socialstyrelsen har sedan 2014 följt den digitala utvecklingen i kommunerna som även berör vissa frågor om socialtjänstens informationssäkerhetsarbete.

det upp till kommunerna att använda sig av resultaten i sin verksamhetsutveckling.[274] Socialstyrelsen har bedömt att ett utökat nationellt stöd kan främja de konstaterade bristerna i framför allt mindre kommuner.[275] Socialstyrelsen har inte specificerat vilket stöd som behövs eller vilken nationell aktör som bör tillhandahålla detta stöd i sin rapport till regeringen.[276] Enligt Socialstyrelsen har myndigheten inte ett uttryckligt uppdrag att följa informationssäkerhetsarbetet, utan det har de gjort på eget initiativ.[277]

Enligt Socialdepartementet har regeringen inte haft diskussioner med Socialstyrelsen om deras förslag på nationellt stöd. Däremot har frågan diskuterats på tjänstemannanivå, och då har det handlat om att mindre kommuner saknar tillräcklig kompetens och tillräckliga resurser för att åtgärda kända brister. Socialstyrelsens återrapportering var ett av underlagen till regeringens beslut om att stödja SKR:s stödfunktion under 2023 (avsnitt 3.5) och till beslutet om statsbidrag till kommuner som kunde användas för bland annat informationssäkerhet (avsnitt 3.3.5).[278]

3.3.7 ... men undersöker inte behovet av stöd

Företrädare för Socialstyrelsen framhåller att de eftersträvar att ta fram stöd som så långt som möjligt är anpassat efter målgruppernas behov.[279] Socialstyrelsen har dock inte undersökt vilket stöd vården och omsorgen behöver när det gäller informationssäkerhet. Dessutom har Socialstyrelsen inte undersökt om deras föreskrifter och handbok[280] möter vårdens behov av stöd. Enligt rättsavdelningen får Socialstyrelsen vissa indikationer på behovet av förbättringar i sina föreskrifter genom möten och konferenser med olika aktörer. Trots regelbundna kontakter med SKR och IVO tas informationssäkerhet sällan upp som en separat punkt.[281]

3.4 Stödet vid allvarliga incidenter är begränsat

IMY ger inte operativt stöd vid allvarliga personuppgiftsincidenter och MSB ger sällan operativt stöd vid allvarliga IT-incidenter till vårdgivare. Vård- och omsorgsgivare som drabbas av allvarliga IT-incidenter, till exempel cyberangrepp, tar oftast stöd av privata konsulter för att lindra effekterna av det inträffade. Omsorgsgivare, som inte omfattas av NIS-lagen, kan söka stöd hos MSB men är beroende av myndighetens prioriteringar för att kunna få stöd.

274 Intervju med företrädare för Socialstyrelsen, 2023-04-05.
275 Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2023*, 2023, s. 8.
276 Socialstyrelsens svar på skriftliga frågor, 2023-09-22.
277 E-post från Socialstyrelsen, 2024-02-12.
278 Regeringskansliets svar på skriftliga frågor, 2023-10-03.
279 Socialstyrelsens svar på skriftliga frågor, 2023-09-22.
280 Här avses främst föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården samt tillhörande handbok.
281 Intervju med företrädare för rättsavdelningen på Socialstyrelsen, 2022-11-24.

3.4.1 MSB ger sällan operativt stöd vid allvarliga IT-incidenter

MSB:s CERT-funktion ska agera skyndsamt vid IT-incidenter genom att sprida information och vid behov samordna åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av det inträffade.[282] Det kan exempelvis gälla vid cyberangrepp. Såväl vård- som omsorgsgivare kan anmäla IT-incidenter till MSB som erbjuder stöd i mån av tid och resurser. MSB prioriterar vårdgivare som bedriver samhällsviktig verksamhet enligt NIS-lagen.[283]

Vår granskning visar att antalet fall där MSB gett operativt stöd för att lindra effekterna av inträffade incidenter är få. MSB ger framför allt råd om hur incidenten kan hanteras utifrån tidigare erfarenheter eller annan information. Enligt MSB är det dock den enskilda verksamheten som måste hantera konsekvenserna av en inträffad IT-incident i sina system eftersom den har tillgång till de specifika systemen och detaljkunskaper om IT-miljöns utformning, komponenter och konfiguration. MSB anser att de har svårt att ge operativt stöd utan att ha den kunskapen.[284]

Riksrevisionen har granskat information från MSB och två kommuner som drabbades av cyberangrepp i december 2022.[285] I dessa fall följde MSB de krav som NIS-förordningen ställer genom att ta emot anmälningar och hålla kontakt med verksamheterna. Båda kommunerna hanterade de direkta konsekvenserna av cyberangreppet i sina IT-system med hjälp av privata konsultföretag eftersom MSB inte kan ge sådant stöd. Sådan hantering kan vara kostsam och kommunen som vi har intervjuat uppger att de betalade drygt 2,5 miljoner kronor för att hantera de akuta konsekvenserna av angreppet.

I granskningen framkommer också att det kan vara oklart vilket stöd MSB kan bidra med vid cyberangrepp. En kommun som drabbats av cyberangrepp hade förväntningar om att MSB kunde bidra med mer operativt stöd än vad myndigheten gjorde.[286]

3.4.2 IMY ger inte stöd vid personuppgiftsincidenter

När verksamheter, däribland vårdgivare eller omsorgsgivare, anmäler personuppgiftsincidenter till IMY kan de inte få stöd i att hantera dem, till exempel vid allvarliga händelser såsom ett cyberangrepp.[287] Enligt IMY beror det på att myndigheten inte har i uppdrag att ge sådant stöd. IMY kommer sällan i kontakt med verksamheten som har anmält incidenten förrän en eventuell tillsyn inleds, vilket

282 11 b § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.
283 MSB:s svar på skriftliga frågor 2023-10-06.
284 Intervju med företrädare för MSB, 2022-12-12 och 2022-12-16.
285 Intervju med företrädare för kommun 7. Vi har kontaktat den andra kommunen men inte genomfört någon intervju. Informationen om det inträffade kommer enbart från MSB.
286 MSB:s svar på skriftliga frågor, 2023-10-06.
287 Humana AB, som bedriver omfattande omsorgsverksamhet, utsattes i mars 2023 för ett dataintrång och angriparen kunde stjäla bland annat känsliga personuppgifter. Se Humana, ”IT-angrepp från tredje part”, hämtad 2023-03-07.

sker mycket sällan. Företrädare för IMY anser att det behövs en stödfunktion som den drabbade verksamheten snabbt kan komma i kontakt med eftersom det är viktigt att vidta åtgärder så tidigt som möjligt vid ett cyberangrepp.[288]

3.5 SKR:s stöd till vård- och omsorgsgivares informationssäkerhetsarbete

Kommunerna har nytta av SKR:s Klassa-verktyg för klassificering av information. Men de kommuner som intervjuats i granskningen upplever inte att SKR i övrigt ger tillräckligt med stöd till deras informationssäkerhetsarbete. Nätverket som SKR driver är värdefullt för övergripande diskussioner men har begränsad praktisk nytta för informationssäkerhetsarbetet, enligt de intervjuade kommunerna.

SKR tillhandahåller verktyget Klassa för klassificering av information som ska skyddas i vård och omsorg. Alla intervjuade kommuner använder och har nytta av verktyget när de klassificerar information efter hur allvarliga konsekvenserna skulle bli av bristande informationssäkerhet. Två kommuner betonar att verktyget är konkret, bland annat eftersom den ger förslag på säkerhetsåtgärder utifrån lagrum.[289]

Inom ramen för en överenskommelse med regeringen[290] skapade SKR stödfunktionen Kompetenscentrum Välfärdsteknik. Ett syfte var att ge råd, stöd och vägledning i frågor om bland annat informationssäkerhet. Myndigheten för vård- och omsorgsanalys (Vård- och omsorgsanalys) som utvärderat överenskommelsen konstaterade att stödfunktionen har stöttat kommunerna i praktiska verksamhetsfrågor men inte prioriterat stöd för övergripande och strukturella frågor såsom informationssäkerhet. Socialcheferna understryker att kompetenscentret har haft begränsad påverkan på deras arbete med informationssäkerhet, särskilt när det gäller IT-säkerhet. Vård- och omsorgsanalys konstaterade också att samverkan rent allmänt mellan SKR och myndigheterna var begränsad och inte fungerade effektivt.[291] I vår granskning uppger majoriteten av de intervjuade kommunerna att de inte känner till SKR:s stödfunktion.[292] Överenskommelsen omfattade också tilldelning av medel, men endast 10 procent av kommunerna använde medlen för sitt informationssäkerhetsarbete.[293]

---

288 Intervju med företrädare för IMY, 2023-05-02 och e-post från IMY, 2024-02-14.

289 Intervju med företrädare för kommun 1 och kommun 4.

290 Överenskommelsen om äldreomsorg – teknik, kvalitet och effektivitet med den äldre i fokus.

291 Myndigheten för vård- och omsorgsanalys, *Digital potential - Utvärdering av satsningen på digital teknik i äldreomsorgen*, 2023, s. 43, 60, 128, rapport 2023:6.

292 Intervju med företrädare för kommun 1, kommun 2, kommun 3 och kommun 5.

293 Cirka 10 procent av kommunerna uppger att de har använt delar av medlen för bland annat utrustning eller system för säker identitet och behörighetsidentifikation som stärker informationssäkerheten. Se Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2022*, 2022, s. 71–72 och e-post från Socialstyrelsen, 2024-02-12

SKR bedriver också nätverk för informationssäkerhet i regioner och kommuner.[294] Ett av dessa är KIS som riktar sig till dem som ansvarar för informationssäkerhetsarbetet i kommunerna. Enligt SKR deltar cirka 180 av 290 kommuner. En intervjuad kommun anser att nätverket ger relevant övergripande information men att det är svårt att föra över kunskapen till personalen som hanterar informationen i verksamheterna.[295] Två andra kommuner anser att nätverken fungerar bra som omvärldsbevakning och som forum för diskussioner men att nyttan är begränsad. Diskussionerna är på övergripande nivå och handlar främst om utmaningar.[296]

3.6 Regeringen har vidtagit få åtgärder för att stärka vårdens och omsorgens informationssäkerhet

Regeringens åtgärder har fokuserat på det generella stödet för samhällets informationssäkerhetsarbete. För att stärka informationssäkerhetsarbetet i kommunerna har regeringen ingått överenskommelser med SKR (avsnitt 3.5.), fattat beslut om statsbidrag (avsnitt 3.3.5.) och tillsatt utredningar. Regeringen har dock vidtagit få särskilda åtgärder för att stödet till vården och omsorgen ska bli mer anpassat till de behov som finns inom sektorn.

3.6.1 Regeringens arbete för att stärka samhällets informations- och cybersäkerhet har inte varit effektivt

Regeringen antog en nationell strategi för samhällets informations- och cybersäkerhet 2017, som riksdagen ställde sig bakom. Ett huvudsyfte var att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet.[297] Riksrevisionen konstaterade i en granskning från 2023 att regeringens arbete för att stärka samhällets informations- och cybersäkerhet inte har varit effektivt. Den centrala bristen är avsaknad av strategiska avvägningar och prioriteringar som inriktar arbetet. Riksrevisionen konstaterade också att strategin saknar en tydlig vision, uppföljningsbara målsättningar, ansvariga för att genomföra åtgärder och tilldelade resurser för arbetet. Det saknas i stort resonemang om målsättningar eller åtgärder kopplat till olika aktörer eller sektorer. Sammantaget gör detta att departement och myndigheter arbetar utifrån sina respektive mål och prioriteringar. Enligt Riksrevisionen riskerar det att leda till att de åtgärder som vidtas inte får effekt, men också till ett ineffektivt resursutnyttjande.[298]

Regeringen ansåg vidare i strategin att en nationell modell för informations- och cybersäkerhet bör tas fram för att stärka informationssäkerhetsarbetet hos samhällets aktörer. Denna syftar till att underlätta för aktörer att göra mer enhetliga

[294] Hälso- och sjukvårdens informationssäkerhetsnätverk (HoSIS) är ett nätverk för regionernas och privata vårdgivares informationssäkerhetsansvariga.
[295] Intervju med företrädare för kommun 2.
[296] Intervju med företrädare för kommun 1 och kommun 6.
[297] Skr. 2016/17:213 s. 8, bet. 2017/18:FöU4, s. 15, rskr 2017/18:142.
[298] Riksrevisionen, *Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023, s. 4.

bedömningar av risker, hot och säkerhetsåtgärder,[299] vilket enligt Riksrevisionens granskning skulle kunna bidra till att skapa en grundnivå för säkerhetsåtgärder. Men någon nationell modell har inte tagits fram.[300] Regeringskansliet har inlett arbetet med att ta fram en ny informations- och cyberssäkerhetsstrategi.[301]

3.6.2 Regeringen har fokuserat på att stärka det generella stödet för samhällets informationssäkerhet

Regeringen gav 2018 i uppdrag till bland annat MSB[302] att ta fram en samlad handlingsplan för arbetet med samhällets informations- och cybersäkerhet utifrån målen i nationella strategin. Handlingsplanen gällde för åren 2019–2022.[303] Regeringen gav 2018 också MSB i uppdrag att utveckla metodstödet för systematiskt informationssäkerhetsarbete och att genomföra utbildningsinsatser till kommuner och regioner.[304] Regeringen gav även MSB i uppdrag 2022 att stärka sitt stöd för aktörers arbete med att förebygga och hantera IT-incidenter samt att utveckla och förenkla stödet för informations- och cybersäkerhet.[305] (Se avsnitt 3.1.1.) För att stärka MSB:s stöd till drabbade aktörer vid IT-incidenter utökade regeringen MSB:s anslag med 20 miljoner kronor för 2024.[306]

På uppdrag av regeringen har MSB reviderat sina föreskrifter om informationssäkerhet för statliga myndigheter, och tagit fram nya föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, med tillhörande vägledning för att underlätta tillämpning.[307]

3.6.3 Flera utredningar berör informationssäkerhet

Regeringen har tillsatt utredningar som berör delning av data och dataanvändning samt informationssäkerhet inom vård och omsorg.

Regeringen tillsatte i juni 2022 en utredning för att analysera och föreslå åtgärder för en bättre och säkrare informationsförsörjning av hälsodata mellan system och aktörer i vården och omsorgen. Utredningen skulle bland annat redovisa hur föreslagna åtgärder förhåller sig till informationssäkerhet.[308] Utredningen lämnade ett delbetänkande i december 2023 och bedömer att det finns en rättslig osäkerhet bland hälso- och sjukvårdens aktörer om hur olika bestämmelser för att hantera information ska tolkas. Denna osäkerhet har enligt utredningen i många fall lett till felaktiga uppfattningar om rättsliga hinder för hantering och delning av information,

299 Bet. 2017/18:FöU4, s. 8.
300 Riksrevisionen, *Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023, s. 34–36.
301 Regeringskansliets svar på skriftliga frågor, 2023-10-03.
302 Även följande myndigheter omfattades av uppdraget: Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen.
303 Regeringsbeslut, 2018-07-12 Ju2018/03737/SSK.
304 Regeringsbeslut (Ju2018/02265).
305 Regeringsbeslut (Ju2022/02219).
306 Prop. 2023/24:1 Utgiftsområde 6, s. 96.
307 Regeringskansliets svar på skriftliga frågor, 2023-10-03.
308 Dir. 2022:98.

och till att olika aktörer gör olika bedömningar. Utredningen bedömer att aktörerna inom hälso- och sjukvården bör erbjudas stöd för att tolka och tillämpa lagreglerna. Utredningen föreslår att E-hälsomyndigheten ska få i uppgift att samordna de statliga myndigheternas stöd och vägledning i juridiska frågor rörande hanteringen av information för hälso- och sjukvårdens digitalisering.[309]

Europaparlamentet och rådet antog 2022 två nya EU-direktiv: direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) och direktivet om kritiska entiteters motståndskraft (CER-direktivet). Regeringen tillsatte i februari 2023 en utredning för att föreslå de anpassningar av svensk rätt som är nödvändiga för att direktiven ska kunna genomföras.[310] Utredningen om genomförande av NIS2- och CER-direktiven lämnade ett delbetänkande den 5 mars 2024 och föreslår att NIS2-direktivet införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare NIS-lagen upphävs. NIS2-direktivet skärper kraven för verksamhetsutövare och syftet är att uppnå en högre cybersäkerhet. Utredningen föreslår därför att fler verksamheter och sektorer ska omfattas av den föreslagna cybersäkerhetslagen och att bestämmelserna ska gälla för hela verksamheten och inte bara för samhällsviktiga och digitala tjänster. Utredningen föreslår att kommuner ska omfattas av lagen. Bestämmelserna innebär bland annat att verksamhetsutövare ska vidta åtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Det ställs också krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete samt att verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning.[311] Eftersom kommunen som sådan – frånsett kommunfullmäktige – föreslås omfattas av de nya bestämmelserna kan det även innebära att omsorgsgivare omfattas av bestämmelserna i viss utsträckning. Verksamhetsutövare av omsorg omfattas dock inte explicit av bestämmelserna. Riksrevisionen bedömer att tillämpningsområdet för bestämmelserna behöver förtydligas när det gäller omsorgsgivare i det fortsatta lagstiftningsarbetet som pågår i Regeringskansliet.

3.6.4 Det saknas tydlig reglering av säkerhetsåtgärder för socialtjänstens personuppgiftsbehandling

Inom vården finns reglering om säkerhetsåtgärder i PDL men motsvarande bestämmelser saknas i lagstiftningen som reglerar socialtjänstens personuppgiftsbehandling, trots att socialtjänsten behandlar personuppgifter som är känsliga på samma nivå som de personuppgifter som behandlas inom vården.[312] Nya bestämmelser som trädde i kraft den 1 mars 2024 ställer krav på omsorgsgivare att arbeta systematiskt med behörighetstilldelning och kontroll.[313]

309 SOU 2023:83.

310 Utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (Fö 2023:01).

311 SOU 2024:18, s. 15–18.

312 Socialstyrelsen 2019, *Säker personuppgiftsbehandling i socialtjänsten*, s. 7.

313 Se 10 § lagen om behandling av personuppgifter inom socialtjänsten, prop. 2022/23:131, bet. 2023/24:SoU3, rskr. 2023/24:46.

Sedan den 1 januari 2023 kan vård- och omsorgsgivare på frivillig basis dela personuppgifter elektroniskt enligt lagen om sammanhållen vård- och omsorgsdokumentation. För att kunna göra det krävs att journalsystemen har inbyggda funktioner för identifiering, behörighetskontroll och loggning. De vård- och omsorgsgivare som ansluter sig omfattas av bestämmelser i lagen som till viss del innebär att kraven på skydd av personuppgifter ökar för omsorgsgivare. Det handlar främst om tilldelning av behörighet för intern elektronisk åtkomst och kontroll av elektronisk åtkomst till personuppgifter.

För att bland annat regleringarna om säkerhetsåtgärder inom vissa delar av äldreomsorgen och vården ska bli mer lika antog riksdagen regeringens proposition 2022/23:131 Välfärdsteknik inom äldreomsorgen. Genom ändringen, som trädde i kraft den 1 mars 2024, införs bestämmelser i lagen om behandling av personuppgifter inom socialtjänsten som tydliggör vilka säkerhetsåtgärder som ska finnas för att kraven i dataskyddsförordningen ska uppfyllas vid användningen av vissa välfärdstekniker.[314] Riksrevisionen konstaterar dock att detta inte kommer att medföra en generell förstärkning av skyddet för personuppgifter inom socialtjänsten eller ens alla biståndsinsatser som är riktade mot äldre. Ändringen avser vissa krav på behörighetstilldelning och kontroll av sådana behörigheter. När det gäller säkerhetsåtgärder avser ändringen endast bistånd i form av hemtjänst eller boende i särskilda boendeformer för äldre och vid användning av digital teknik. Lagrådet ifrågasatte begränsningen till en del av verksamheten och konstaterade att den osäkerhet som kommuner uttryckt angående lagstödet för att använda digital teknik generellt kommer att kvarstå.[315]

[314] Prop. 2022/23:131.

[315] Lagrådet ifrågasatte även skälen som angavs för att begränsa förslagen till att avse bistånd i form av hemtjänst eller boende i särskilda boendeformer för äldre. För att utgöra ett klarläggande bör en reglering av detta slag omfatta all användning av digital teknik vid biståndsinsatser. För en sådan reglering saknades beredningsunderlag i ärendet.

4 Tillsyn av vårdens och omsorgens informationssäkerhet

I detta kapitel besvaras den andra delfrågan: Är myndigheternas tillsyn av vårdens och omsorgens informationssäkerhet effektiv? Detta är våra viktigaste iakttagelser:

- IMY har sedan 2018 genomfört begränsad tillsyn av vårdgivares informationssäkerhetsarbete och ingen tillsyn av omsorgsgivares. Bidragande orsaker är ökat fokus på hantering av klagomål från enskilda och ineffektiv handläggning med årslånga handläggningstider.
- IVO bedriver ingen tillsyn av omsorgsgivares informationssäkerhet och sällan av mindre vårdgivares. IVO har dessutom begränsat sin tillsyn enligt NIS-lagen till vårdgivarnas underlag till riskanalyser och åtgärdsplaner. Tillsynen ger därmed inte fullt ut svar på om vårdgivarna har en hög informationssäkerhet och om de bedriver ett systematiskt informationssäkerhetsarbete.
- IVO och IMY har framför allt inriktat tillsynen mot större regionala och kommunala vårdgivare som hanterar stora mängder personuppgifter. Mindre kommunala och enskilda vårdgivare omfattas i mindre utsträckning av tillsyn. IMY inleder också sällan riskbaserad tillsyn och genomför inte systematiska riskanalyser. Det är oklart i vilken utsträckning tillsynen inriktas mot verksamheter där den ger mest nytta.
- IMY och IVO har inte följt upp tillsynens resultat och det är därför oklart vilken effekt tillsynen har på vårdens och omsorgens informationssäkerhet.

4.1 IMY:s tillsyn är delvis riskbaserad och begränsad och tar för lång tid att genomföra

IMY:s tillsyn av informationssäkerheten i vården och omsorgen är i flera avseenden begränsad. IMY har mellan 2018–2022 genomfört begränsad tillsyn av vårdgivares informationssäkerhetsarbete inom vården och ingen alls inom kommunal vård och omsorg. Handläggningstiderna för de avslutade tillsynsärendena är mycket långa. Tillsynen ger därmed ett begränsat bidrag till utvecklingen av praxis, och därmed begränsad vägledning till vårdgivare om vad som krävs av dem för att uppfylla lagens krav. Tillsynen är sällan riskbaserad och utgår främst från klagomål från personer. IMY har inte följt upp tillsynens resultat och det är därför oklart vilken effekt tillsynen har på vårdens informationssäkerhet.

4.1.1 IMY:s tillsyn är delvis riskbaserad och inriktad mot verksamheter där konsekvenserna av brister kan bli störst

IMY har delvis haft ett riskbaserat tillvägagångssätt vid prioritering av den tillsyn som ska genomföras. En konsekvens är att det inte går att avgöra om de prioriterade

områdena och verksamheterna för tillsyn är de med största risker för bristande skydd för personuppgifter, eller om tillsynen gör mest nytta där.

IMY har i urvalet av verksamheter för tillsyn i huvudsak utgått från var konsekvenserna av eventuella brister för skyddet av personuppgifter skulle bli störst, och i mindre utsträckning utgått från vilka verksamheter som har störst brister. Det har resulterat i att tillsynen framför allt inriktats mot större regionala vårdgivare. IMY identifierade och prioriterade regionala vården för tillsyn i sin tillsynsplan för 2019–2020. Kommunal vård och omsorg som hanterar liknande känsliga personuppgifter och har betydande brister i sitt informationssäkerhetsarbete sågs inte som ett riskområde.[316] Vare sig vården eller omsorgen identifierades som prioriterade riskområden i tillsynsplanerna för 2021–2023.[317] Anledningen till detta är enligt IMY är att de behövde göra prioriteringar på grund av underfinansierad verksamhet.[318]

IMY har inte dokumenterat riskanalyserna eller underlagen som använts för att välja tillsynsobjekt.[319] Det försvårar insyn i vilka källor analysen bygger på, vilka problem och risker inom informationssäkerhet som IMY anser vara störst, vilka sektorer som är mest drabbade och hur IMY har prioriterat bland dessa risker och sektorer.

Vår genomgång av IMY:s genomförda tillsynsärenden inom vården 2018–2022 visar att ärendena var delvis riskbaserade och delvis händelsestyrda. IMY:s tillsyn av åtta vårdgivare i mars 2019 utgick från tidigare erfarenheter och kunskap om risker.[320] De övriga tillsynsärendena inleddes direkt efter medierapportering om risker eller efter personuppgiftsincidenter och klagomål. Sådana tillsynsärenden har vi sett som händelsestyrd tillsyn, till exempel tillsynen av 1177 och av Region Uppsala.

IMY bedömer riskområden utifrån en samlad bild av personuppgiftsincidenter, klagomål och omvärldsbevakning. Vid riskbaserad tillsyn ska IMY ta hänsyn till faktorer som behov av vägledande praxis, ny teknik och konsekvenser för många.[321] IMY har inte beaktat rapporter från Socialstyrelsen eller MSB som identifierar brister i regioners och kommuners informationssäkerhet. IMY har inte heller analyserat mörkertalet av personuppgiftsincidenter för att rikta tillsynen mot de vård- och omsorgsgivare som inte rapporterar eller som sällan gör det.[322]

IMY:s mål är att tillsynen ska etablera praxis och främja lärande, genomföras effektivt och rättssäkert och ha en positiv effekt på individuella ärenden och samhällets integritetsskydd. IMY har inte satt specifika kvantitativa mål för antalet

316 Datainspektionen, *Tillsynsplan 2019–2020,* 2019.
317 IMY, *Tillsynsplan 2021–2022,* 2021 och IMY, *Tillsynsplan 2023,* 2023.
318 Intervju med företrädare för IMY, 2023-03-30.
319 Intervju med företrädare för IMY, 2023-03-08.
320 Se IMY, ”Brister i hur vårdgivare styr personalens åtkomst till journaluppgifter” för besluten, hämtad 2023-11-15.
321 IMY, *Tillsynsplan 2021–2022,* 2021 och IMY, *Tillsynsplan 2023,* 2023.
322 Intervju med företrädare för IMY, 2023-03-30.

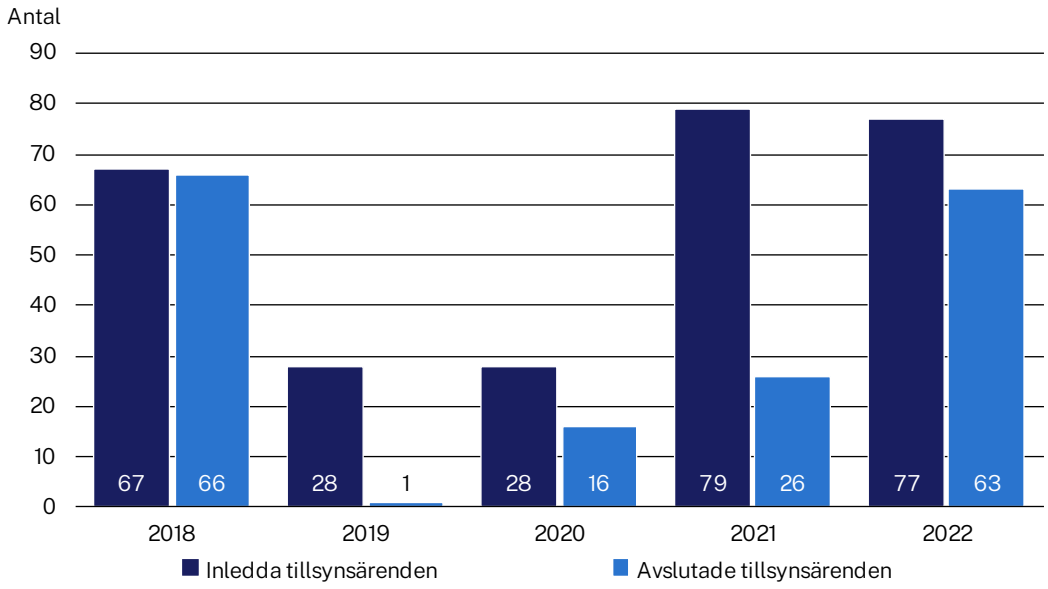
tillsynsärenden eller resurserna för tillsynen. I stället siktar IMY på att initiera och avsluta fler tillsynsärenden jämfört med föregående år.[323]

4.1.2 Begränsad tillsyn av vårdens informationssäkerhet och ingen av omsorgens

Mellan 2018 och 2022 genomförde IMY ett fåtal tillsynsärenden av vårdgivarnas informationssäkerhet inom vården, och inga alls inom kommunal vård och omsorg.[324] En konsekvens av detta är att tillsynen inte i tillräcklig utsträckning bidrar till att skapa praxis och därigenom stärka informationssäkerheten.

Totalt inledde IMY 279 och avslutade 172 tillsynsärenden enligt dataskyddsförordningen i alla sektorer (se diagram 1). När det gäller tillsynsärenden inom vården inledde IMY 16 och avslutade 14 tillsynsärenden under samma period. I de flesta fallen ledde besluten av tillsynsärenden inom vården till sanktionsavgifter på mellan 250 000 kronor och 30 miljoner kronor.[325] Under 2022 inledde IMY tillsyn av tre vårdgivare men ingen av dessa avslutades under året.[326]

Diagram 1 Antal tillsynsärenden enligt dataskyddsförordningen i alla sektorer, 2018–2022



Källa: IMY:s årsredovisningar för 2021 och 2022.

323 IMY, *IMY:s mål- och resultatkarta,* 2021. IMY har satt mål för handläggningstider, se avsnitt 4.1.3.

324 Dåvarande Datainspektionen inledde tillsyn av Omsorgsnämnden och äldrenämnden i Uppsala kommun i februari 2017. Man undersökte behörighetstilldelning och loggkontroller i journalsystemet och fann flera brister. Beslut fattades i juni 2019.

325 Tillsynen har omfattat offentliga och enskilda vårdgivare.

326 Tillsyn av Kry International AB, Region Uppsala och Region Skåne.

IMY anser att de inte har uppnått målet om fler tillsynsärenden och att det huvudsakligen beror på att myndigheten har inlett och avslutat för få tillsynsärenden inom dataskydd.[327] Trots en ökning mellan 2020 och 2022 anser IMY att det totala antalet tillsynsärenden var betydligt lägre än förväntat. Det beror på att större delen av tillsynen var baserad på klagomål från personer som ansåg att deras personuppgifter behandlades felaktigt,[328] snarare än på planerad eller riskbaserad tillsyn vilket minskade avsevärt under samma period.[329] Till skillnad från riskbaserad tillsyn är den klagomålsbaserade tillsynen av begränsad omfattning[330] eftersom den bara fokuserar på de brister som klaganden framför. De flesta klagomål handlar om att enskildas rättigheter enligt dataskyddsförordningen inte blivit tillgodosedda, till exempel rätten till radering av personuppgifter från register. En mindre del av klagomålen handlar om säkerhetsbrister, till exempel att personuppgifter har skickats i okrypterade mejl.[331] Klagomålsbaserad tillsyn ger därför begränsad effekt på informationssäkerhetsarbetet.

IMY har prioriterat klagomålsbaserad tillsyn på grund av ett beslut från EDPB, vilket innebär att IMY sedan 2021 anser att de måste bedöma varje klagomål och inleda tillsyn vid behov. Detta har lett till att IMY behöver bedöma drygt 2 000 enskilda klagomål årligen, vilket enligt IMY är mycket resurskrävande.[332] Under 2023 ökade antalet inkomna klagomål med nästan 50 procent.[333]

För att hantera klagomålen har IMY flyttat resurser från andra verksamhetsområden vilket har påverkat deras förmåga att inleda och avsluta tillsynsärenden i tid. IMY har inte klarat av att utreda alla klagomål i tid och inleda all tillsyn som borde ha inletts. Sedan 2020 har IMY ackumulerat stora ärendebalanser[334] inom klagomåls- och tillsynsverksamheten.[335] Enligt IMY beror obalanser främst på gränsöverskridande klagomål som kräver samverkan med andra dataskyddsmyndigheter.[336] Den genomsnittliga handläggningstiden för klagomål ökade från 11 dagar 2020 till 73 dagar 2022. Denna ökning beror enligt IMY främst på de gränsöverskridande klagomålen och bristande resurser.[337]

---

327 IMY, *Årsredovisning 2021*, 2022, s. 45 och IMY, *Årsredovisning 2022*, 2023, s. 26 och intervju med företrädare för IMY, 2023-03-30.

328 IMY, *Årsredovisning 2021*, 2022, s. 17, 41–42, IMY, *Årsredovisning 2022*, 2023, s. 23–26 och intervju med företrädare för IMY, 2023-03-30.

329 Intervju med företrädare för IMY, 2023-03-30 och IMY, *Integritetsskyddsmyndighetens budgetunderlag 2023–2025*, 2022, s. 7.

330 Tillsyn i kategori 1 och 2 är enklare och mindre omfattande tillsynsärenden med enbart skriftväxling med tillsynsobjektet. I gränsöverskridande klagomålsärenden tillkommer också skriftväxling med andra berörda tillsynsmyndigheter. Kategori 3 är ärenden som kräver en större rättsutredning eller fler utredningsåtgärder än enbart kommunikation med tillsynsobjektet. Till kategori 4 hör de mest komplexa ärendena som omfattar inspektion.

331 IMY, *Klagomål till IMY - den nationella bilden 2021*, 2022.

332 Intervju med företrädare för IMY, 2023-03-30 och IMY, *Årsredovisning 2022*, 2023, s. 21–22.

333 IMY, *Årsredovisning 2023*, 2024, s. 27.

334 Klagomåls- och tillsynsärenden som fortfarande är under handläggning.

335 Intervju med företrädare för IMY, 2023-03-30, IMY:s svar på skriftliga frågor, 2023-10-04 och IMY, *Integritetsskyddsmyndighetens budgetunderlag 2022–2024*, 2021 ¸ s. 18–20.

336 IMY, *Integritetsskyddsmyndighetens budgetunderlag 2022–2024*, 2021, s. 7.

337 IMY, *Årsredovisning 2022*, 2023, s. 22–23 och IMY:s svar på skriftliga frågor, 2023-10-04.

IMY anser att deras organisation behöver blir mer effektiv. För att minska obalanser och handläggningstider för klagomålen planerar IMY att förbättra sina arbetsprocesser och öka erfarenhetsutbyte och kompetensen bland personalen.[338]

Kommuner som vi har intervjuat vill ha tillsyn av sitt informationssäkerhetsarbete. Bland dem ser två mindre kommuner tillsynen som ett sätt att få vägledning i sitt arbete med informationssäkerhet.[339] Två större kommuner betonar att tillsyn skulle öka ledningens engagemang och att informationssäkerhetsarbetet prioriteras.[340]

4.1.3 Det tar mycket lång tid att genomföra tillsyn

Handläggningstiderna för de avslutade tillsynsärendena är mycket långa och är en viktig förklaring till varför IMY inte kan inleda och avsluta fler tillsynsärenden.[341] Under 2022 var den genomsnittliga handläggningstiden för avslutade tillsynsärenden[342] 223 dagar, jämfört med 321 dagar under 2021 och 319 dagar under 2020. Den minskade tiden under 2022 berodde på att IMY avslutade många tillsynsärenden som var enklare och inte så omfattande.[343] För dessa enklare ärenden (kategori 1 och 2) var handläggningstiden 121 dagar, medan mer omfattande och komplexa ärenden såsom riskbaserad tillsyn (kategori 3 och 4) tog 824 respektive 760 dagar,[344] vilket är långt över IMY:s egna mål.[345]

IMY:s tillsyn av vårdgivarna under 2019 tog ännu längre tid, från cirka 630 till 960 dagar. Dessa tillsynsärenden tillhörde kategori 3 och 4.

4.1.4 Försiktighet vid tolkning av bestämmelserna bidrar till långa handläggningstider

IMY behöver ofta fatta beslut som kan få större genomslag än för det enskilda ärendet. Det finns begränsad domstolspraxis och vägledning från EDPB, vilket gör att IMY behöver tolka dataskyddsbestämmelserna och ta ställning i rättsliga frågor.

Våra intervjuer med företrädare för IMY visar att de fokuserar mycket på rättssäkerhet och är försiktiga med att tolka dataskyddsförordningen, och att de sällan gör rättsliga ställningstaganden i frågor där det saknas praxis eller vägledning. Bristen på rättsliga ställningstaganden minskar myndighetens förmåga att snabbt avgöra rättsliga frågor och leder till att de spenderar betydande tid på interna diskussioner

338 IMY:s svar på skriftliga frågor, 2023-10-04.
339 Intervju med företrädare för kommun 2 och kommun 5.
340 Intervju med företrädare för kommun 1 och kommun 6.
341 Intervju med företrädare för IMY, 2023-03-30.
342 Den genomsnittliga handläggningstiden omfattar tillsynen enligt dataskyddsförordningen, brottsdatalagen och kamerabevakningslagen.
343 IMY, *Årsredovisning 2022*, 2023, s. 26.
344 Uppgifterna enligt de fyra kategorierna avser de genomsnittliga handläggningstiderna under 2021. IMY har inte redovisat motsvarande uppgifter för 2022.
345 Målet för handläggningstid i kategori 1 och 2 är 90 dagar, 180 dagar i kategori 3 och 360 dagar i kategori 4. Se IMY, *IMY:s mål- och resultatkarta*, 2021.

och rättsutredningar för att förankra beslut.[346] IMY har sedan 2020 arbetat med att utveckla och effektivisera sin verksamhet och tillsynsprocessen men detta har inte resulterat i kortare handläggningstider.[347] Antalet avslutade tillsynsärenden per årsarbetskraft i slutet av 2021 låg enligt IMY på en fortsatt mycket låg nivå.[348].

Andra orsaker som begränsar kapaciteten att inleda och avsluta fler tillsynsärende med kortare handläggningstider är enligt IMY brist på finansiering och resurser, stor personalomsättning och resurskrävande överklaganden av besluten.[349] Regeringen är medveten om att IMY har prioriterat ned den riskbaserade tillsynen och att handläggningstiderna och ärendebalanserna har ökat inom en del ärendekategorier. Enligt företrädare för Justitiedepartementet är IMY fullständigt oberoende och regeringen är därför restriktiv i sin styrning av myndigheten.[350] För att stärka IMY:s förmåga att bedriva sin verksamhet höjde regeringen IMY:s ramanslag från cirka 124 miljoner kronor år 2022 till ungefär 172 miljoner kronor år 2023. IMY anser att det ökade anslaget kommer att leda till minskade ärendebalanserna och handläggningstider för tillsyn vid utgången av 2024.[351] Sedan november 2023 har de som lämnat in klagomål till IMY rätt att överklaga besluten, enligt Högsta förvaltningsdomstolens avgöranden. IMY har bedömt att myndigheten blir part i IMY:s klagomåls- och tillsynsärenden. Enligt IMY kommer myndigheten att behöva inleda tillsyn i betydligt fler klagomålsärenden än tidigare, vilket kommer vara resurskrävande och leda till längre handläggningstider. För att hantera detta mer effektivt uppger IMY att de ska införa nya rutiner, digitala verksamhetsstöd och processer för klagomåls- och tillsynshantering under våren 2024.[352]

En annan orsak som påverkar kapaciteten är att juristerna som arbetar med tillsynsärenden också har fått arbeta med klagomålshantering, remisser, förhandsamråd, tillstånd, samverkansfrågor och svar på olika frågor från enskilda och verksamheter. För att använda personalens tid och förmåga mer effektivt har enheter för tillsyn sedan april 2023 i första hand arbetat med tillsyn, klagomål och tillstånd.[353]

4.1.5 IMY följer inte upp resultaten av sin tillsyn

IMY följer inte upp att de verksamheter som varit föremål för tillsyn faktiskt vidtar de åtgärder som IMY har förelagt i tillsynsbesluten. Enligt IMY beror det på att många av IMY:s tillsynsbeslut har överklagats och inte vunnit laga kraft, vilket inte möjliggör

346 Intervju med företrädare för IMY, 2022-12-01, intervju med företrädare för IMY, 2023-03-30, intervju med företrädare för IMY, 2023-04-24 och IMY:s svar på skriftliga frågor, 2023-10-04.

347 IMY, *Integritetsskyddsmyndighetens budgetunderlag 2022–2024*, 2021, s. 8 och intervju med företrädare för IMY, 2023-03-30 och IMY:s svar på skriftliga frågor, 2023-10-04.

348 IMY, *Årsredovisning 2021*, 2022, s. 17, 41–42.

349 Intervju med företrädare för IMY, 2023-03-30 och IMY:s svar på skriftliga frågor, 2023-10-04.

350 Regeringskansliets svar på skriftliga frågor, 2023-10-03.

351 IMY, *Årsredovisning 2022*, 2023 och IMY, *Integritetsskyddsmyndighetens budgetunderlag 2024–2026*, 2023.

352 IMY, *Ställningstagande om partsställning i ärenden som inleds med anledning av klagomål*, 2023.

353 Intervju med företrädare för IMY, 2023-03-30.

uppföljning. IMY saknar en arbetsprocess för att följa upp sina tillsynsbeslut men uppger att de avser att etablera ett sådan process.[354]

4.2 IVO:s tillsyn är begränsad och omfattar vissa delar av informationssäkerheten

IVO:s tillsyn av informationssäkerheten i vården och omsorgen är i flera avseenden begränsad. IVO har inte bedrivit tillsyn av informationssäkerheten i omsorgsverksamheter och mycket sällan i de mindre vårdverksamheter som inte omfattas av NIS-lagen.[355] Den tillsyn som IVO bedriver av vårdgivares informationssäkerhet enligt NIS-lagen omfattar i huvudsak verksamheternas riskanalyser och åtgärdsplaner. Tillsynen har dock inte kontrollerat om de vidtagna säkerhetsåtgärderna är ändamålsenliga och proportionella för att hantera risker som hotar säkerheten i nätverk och informationssystem. Tillsynen ger därför inte ett fullgott svar på om vårdgivarna har en hög informationssäkerhet och om de bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. Tillsynen ger därmed ett begränsat bidrag till utvecklingen av praxis, och därmed begränsad vägledning till vårdgivare om vad som krävs av dem för att uppnå hög säkerhet i enlighet med lagen. Tillsynen har framför allt inriktats mot större offentliga regionala vårdgivare, medan enskilda vårdgivare och mindre kommunala vårdgivare i mindre utsträckning omfattats av tillsyn. IVO saknar delvis kunskap om utfallet av tillsynen och ger begränsad vägledning inom ramen för enskilda tillsynsärenden.

4.2.1 Tillsynen omfattar inte omsorgsgivare och sällan mindre vårdgivare

IVO har valt att renodla sin tillsyn av informationssäkerhet till att endast gälla NIS-lagen, som omfattar de flesta vårdgivare men inte omsorgsgivare. Anledningen är att NIS-lagen ger IVO ett tydligt ansvar för vissa delar av vårdens informationssäkerhet, att IVO anser att det blir för komplext att fatta beslut om man utgår från flera lagstiftningar samtidigt och att tillsynsbesluten enligt NIS-lagen är möjliga att överklaga.[356]

IVO kan även bedriva tillsyn av informationssäkerhet i vården och omsorgen utifrån annan lagstiftning.[357] Inom omsorgen kan IVO bedriva tillsyn av informationssäkerhet utifrån lagen om behandling av personuppgifter inom socialtjänsten[358] men har aldrig gjort det. Bestämmelserna för omsorgen inte är lika tydliga som de inom vården, vilket enligt IVO begränsar deras möjligheter att bedriva

354 Intervju med företrädare för IMY, 2023-03-30.

355 NIS-lagen omfattar vårdgivare där antalet anställd legitimerad vårdpersonal eller på annat sätt anlitad legitimerad vårdpersonal överstiger 50 årsarbetskrafter, eller där minst 20 000 expedieringar av receptbelagda läkemedel utförs per år. 7 kap. MSB:s föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9).

356 Intervju med företrädare för IVO, 2023-04-20.

357 IVO:s svar på skriftliga frågor, 2023-12-20.

358 Lagen om behandling av personuppgifter inom socialtjänsten.

tillsyn.[359] Dessa skillnader i reglering har även påpekats av Socialstyrelsen.[360] När det gäller tillsyn av vården kan IVO utgå från PDL och Socialstyrelsens föreskrifter om journalföring som omfattar delar av vårdgivarnas informationssäkerhet.[361] Det är dock mycket ovanligt att IVO:s tillsyn av vårdgivare omfattar informationssäkerhet utöver den som görs enligt NIS-lagen.[362]

4.2.2 Tillsynen enligt NIS-lagen omfattar bara vissa delar av vårdgivares informationssäkerhetsarbete

IVO har begränsat sin tillsyn enligt NIS-lagen till delar av vårdgivares informationssäkerhetsarbete. Som skäl anger IVO att det saknas föreskrifter till lagen, som Socialstyrelsen inte har tagit fram. En konsekvens är att tillsynen är begränsad och inte ger ett fullgott svar på om vårdgivarna har en hög informationssäkerhet i vårdgivarnas informationssystem och nätverk där personuppgifter hanteras, och om de bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. En annan konsekvens är att tillsynen ger vårdgivarna begränsad vägledning om vad som krävs av dem för att uppfylla NIS-lagens krav.

NIS-lagen ställer krav på att vårdgivarna ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete för att upprätthålla hög säkerhet i nätverk och informationssystem. IVO:s tillsyn av NIS-lagen omfattar dock i praktiken bara delar av lagens krav.

IVO uppger att det krävs förskrifter med tydligare vägledning för att tillsynen ska kunna omfatta genomförandet av det systematiska informationssäkerhetsarbetet, exempelvis vad som är en ändamålsenlig och proportionell teknisk och organisatorisk åtgärd för att hantera risker som hotar säkerheten i nätverk och informationssystem. IVO menar att de inte kan göra den uttolkningen på egen hand utan föreskrifter. Eftersom Socialstyrelsen inte har tagit fram förskrifter till NIS-lagen har IVO valt att avgränsa sin tillsyn till att i huvudsak granska om vårdgivare tagit fram riskanalyser med tillhörande åtgärdsplaner.[363]

IVO har bedömt att det inte heller går att utgå från andra föreskrifter som omfattar vårdgivares informationssäkerhet i tillsynen. Fram till 2021 utgick IVO från MSB:s föreskrift om informationssäkerhet för leverantörer av samhällsviktiga tjänster[364] när det gäller dokumentation på en generell nivå. Men den är enligt IVO inte tillräckligt anpassad till de komplexa förhållandena i vården för att kunna vara en grund för tillsyn av vårdgivarnas informationssäkerhetsarbete.[365] Socialstyrelsens föreskrifter

359 IVO:s svar på skriftliga frågor, 2023-10-04.
360 Socialstyrelsen, *Säker personuppgiftsbehandling i socialtjänsten. Rättsläge och utgångspunkter,* 2018.
361 Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården.
362 IVO:s svar på skriftliga frågor, 2023-10-04.
363 Intervju med företrädare för IVO, 2023-04-20. IVO:s svar på skriftliga frågor, 2023-12-20.
364 MSB:s föreskrifter och allmänna råd (MSBFS 2018:8) om informationssäkerhet för leverantörer av samhällsviktiga tjänster.
365 IVO:s svar på skriftliga frågor, 2023-12-20.

och allmänna råd om patientsäkerhet respektive ledningssystem för kvalitetsledning[366] är enligt IVO inte heller tillräckligt specifika för att kunna utgöra ett konkret stöd för tillsyn av vårdgivares eller omsorgsgivares informationssäkerhet.[367]

En konsekvens av att IVO begränsat tillsynen enligt NIS-lagen till verksamheternas riskanalyser och åtgärdsplaner är att utvecklingen av praxis begränsas. Därmed begränsas också vägledningen till vårdgivarna om vilka åtgärder de bör vidta i sina informationssystem och nätverk för att leva upp till NIS-lagens krav på hög informationssäkerhet.

IVO har inte påtalat till Regeringskansliet att avsaknaden av föreskrifter till NIS-lagen påverkar tillsynen av informationssäkerhet. Eftersom det pågått en dialog mellan IVO och Socialstyrelsen i frågan har IVO bedömt att den inte behövt lyftas till Regeringskansliet.[368]

4.2.3 IVO har inriktat tillsynen mot verksamheter där konsekvenserna av brister kan bli störst

IVO har i urvalet av verksamheter för tillsyn i huvudsak utgått från var konsekvenserna av eventuella brister i informationssäkerhet skulle bli störst, och i mindre utsträckning utgått från vilka verksamheter som har störst brister. Det har gjort att tillsynen framför allt inriktats mot större offentliga regionala vårdgivare. Mindre kommunala vårdgivare, där bristerna i informationssäkerhet generellt är störst, och enskilda vårdgivare har sällan omfattats av tillsynen.

IVO gör prioriteringar i sin egeninitierade tillsynsverksamhet baserat på en myndighetsövergripande riskanalys. Information från NIS-tillsynen ingår dock inte i denna riskbaserade planering.[369] Inom ramen för NIS-tillsynen gör IVO årligen en riskanalys som resulterar i en årlig tillsynsplan med övergripande prioriteringar för urval av verksamheter för tillsyn. IVO har inte delgett Riksrevisionen denna riskanalys, de underlag som används eller hur den utförs. Enligt IVO baseras riskanalysen på olika interna och externa källor och följer inte en fastställd processbeskrivning.[370] Riskanalysen inom NIS-tillsynen är enligt IVO ett utvecklingsområde.[371]

366 Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2017:40) om vårdgivares systematiska patientsäkerhetsarbete. Socialstyrelsens föreskrifter och allmänna råd (SOSFS 2011:9) om ledningssystem för ett systematiskt kvalitetsarbete.

367 IVO:s svar på skriftliga frågor, 2023-10-04.

368 IVO:s svar på skriftliga frågor, 2023-10-04.

369 IVO:s svar på skriftliga frågor, 2023-10-04.

370 IVO:s svar på skriftliga frågor, 2023-12-20.

371 Intervju med företrädare för IVO, 2023-04-20.

IVO har haft olika utgångspunkter i sina tillsynsplaner.[372] Merparten av de genomförda planerade tillsynsärendena har dock inletts baserat på vårdgivarens storlek och därmed antalet personer som skulle kunna drabbas av en eventuell störning, och inte på vilka verksamheter som har störst brister i informationssäkerheten. I de fall IVO har inlett tillsyn efter inträffade IT-incidenter har tillsynen utgått från den inträffade störningens allvarlighetsgrad och antalet personer som påverkats eller riskerat att påverkas.[373] Det har resulterat i att IVO har prioriterat regionerna och de största kommunerna i tillsynen.[374] Antal tillsynsärenden som gäller vårdgivare enligt NIS-lagen framgår av tabellen nedan.

Tabell 1 Antal tillsynsärenden enligt NIS-lagen per år, januari 2019 - november 2023

År	Antal ärenden totalt	varav regionala vårdgivare	varav kommunala vårdgivare	varav enskilda utförare
2019	23	10	12	1
2020	20	6	12	2
2021	12	5	5	2
2022	11	1	8	2
2023	15	3	12	0
Totalt	**81**	**25**	**49**	**7**
varav unika vårdgivare	65	21	38	6

Källa: Riksrevisionen, bearbetning av uppgifter från IVO. Tandvårdsverksamheter och apotek ingår inte i tabellen. Skillnaden mellan antal ärenden och antal unika vårdgivare beror på att vissa vårdgivare omfattats av flera tillsynsärenden.

Som framgår av tabell 1 omfattas kommunerna i mindre utsträckning av IVO:s tillsyn än regionerna, trots att de generellt har större brister i informationssäkerhet. Mellan januari 2019 och november 2023 täckte IVO in alla regionala vårdgivare i tillsynen och fattade beslut i eller påbörjade tillsyn av 38 kommunala vårdgivare.[375] Det är därmed 34 procent av de kommunala vårdgivare som omfattas av NIS-lagen som till någon del omfattats av tillsyn.[376] Av landets samtliga kommuner är det 13 procent som omfattats av tillsyn, och av de 20 befolkningsmässigt största kommunerna har 16 stycken (80 procent) omfattats av tillsyn.[377]

372 2020 och 2024 hade uppföljning av tidigare beslut högsta prioritet. Under 2021 och 2022 hade incidenter som föranleder tillsyn högsta prioritet. Ej tidigare tillsynade leverantörer prioriterade efter storlek på leverantörens verksamhet (eller motsvarande) hade prioritet 2 under 2020, 4 under 2021, 4 under 2022 och 2 under 2023.

373 IVO:s svar på skriftliga frågor, 2023-12-20.

374 Intervju med företrädare för IVO, 2023-04-20.

375 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20.

376 Antalet unika kommuner som till någon del inlett eller avslutat tillsyn av 2019 till 2023-12-19/ antal kommuner i IVO:s register av samhällsviktiga leverantörer enligt NIS-lagen 2023-12-19. Riksrevisionen, sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20.

377 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20 samt befolkningsuppgifter från Statistiska centralbyrån per 31 december 2022.

IVO har genomfört få tillsynsärenden av informationssäkerhet av enskilda vårdgivare. Sex enskilda vårdgivare har omfattats av tillsyn, varav tre är offentligt ägda bolag.[378] Det innebär att IVO endast genomfört tillsyn av 8 procent av de enskilda vårdgivare som omfattas av NIS-lagen.[379]

4.2.4 Intern resursfördelning och långsam uppbyggnad av NIS-tillsynen har påverkat tillsynens omfattning

Den interna resurstilldelningen och uppbyggnad av kompetens har delvis påverkat antalet genomförda tillsynsärenden mellan 2018 och 2023.

Drygt 200 vårdgivare är anmälda hos IVO som leverantörer av samhällsviktig tjänst och kan därmed bli aktuella för tillsyn enligt NIS-lagen.[380] Omfattningen av tillsynen påverkas av myndighetens prioriteringar av all tillsyn. IVO har anpassat sina interna målsättningar för antalet tillsynsärenden per år efter de resurser som myndigheten internt tilldelat tillsyn enligt NIS-lagen och IVO uppger att de uppsatta målen nås.[381] Som framgår av tabell 1 har IVO genomfört mellan 11 och 15 tillsynsärenden av vårdgivare enligt NIS-lagen per år under de senaste tre åren. Under 2022 var IVO:s kostnader för NIS-tillsynen 8,5 miljoner kronor. Det kan jämföras med vad myndigheten totalt lade på egeninitierade tillsynsärenden inom vård: 104,8 miljoner kronor.[382]

En förklaring till omfattningen av tillsynen är enligt IVO att det tagit tid att rekrytera rätt kompetens. Som en konsekvens använde IVO under 2019 knappt hälften av de 10 miljoner kronor som regeringen tillfört IVO för tillsyn enligt NIS-lagen.[383] Under de första åren efter det att NIS-lagen infördes ägnade IVO också mycket tid åt att identifiera vilka verksamheter som skulle anmäla samhällsviktig tjänst. Enligt IVO dröjde det till 2021 innan myndigheten kommit i fas med det som krävs för tillsyn enligt NIS-lagen.[384]

IVO har för närvarande fyra inspektörer som bedriver NIS-tillsyn på heltid. Även jurister och beslutsfattare deltar i NIS-tillsynen på deltid. Under 2022 avslutade IVO 11 tillsynsärenden som i genomsnitt tog 169 dagar att slutföra. Det innebär att de fyra NIS-inspektörerna genomförde knappt tre tillsynsärenden vardera detta år,[385] trots att tillsynen begränsats till delar av NIS-lagen och i huvudsak utförs som skrivbordstillsyn.

---

378 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20. Bolagen är Attendo Care, Capio, Praktikertjänst, TioHundra AB (ägt av kommuner och region), SOS Alarm (ägt av staten och SKR) och Södersjukhuset i Stockholm (ägt av region).

379 Antalet unika enskilda vårdgivare som IVO till någon del inlett eller avslutat tillsyn av 2019 till 2023-12-19/ antal enskilda vårdgivare i IVO:s register av samhällsviktiga leverantörer enligt NIS-lagen 2023-12-19.

380 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20.

381 IVO:s svar på skriftliga frågor, 2023-12-20. IVO har i ett tidigare skriftligt svar till Riksrevisionen angett att målet för antalet riskbaserade tillsynsärenden är 30–40 per år.

382 IVO, *Årsredovisning 2022*, 2023, s. 62.

383 IVO, *Årsredovisning 2019*, 2020.

384 Intervju med företrädare för IVO, 2023-04-20.

385 Antalet ärenden per antalet NIS-inspektörer varje år.

Som framgår av tabellen nedan sjönk den genomsnittliga handläggningstiden mellan det att ett ärende inleddes och beslutades från 259 dagar under 2021 till 169 dagar under 2022.

Tabell 2 Handläggningstider för tillsynsärenden enligt NIS-lagen per år, 2019–2022

År	Handläggningstid för tillsyn av informationssäkerhetsarbete
2019	261
2020	242
2021	259
2022	169

Handläggningstiderna omfattar dels IVO:s handläggning, dels den väntetid på 30 dagar som IVO ger verksamheterna att inkomma med efterfrågad information.[386] När handläggningstiderna är långa beror det oftast på att IVO behövt begära in många kompletteringar.[387]

4.2.5 Inrapporterade IT-incidenter är sällan grund för tillsyn och IVO analyserar inte mörkertal

IVO inleder sällan tillsyn på grund av inrapporterade IT-incidenter från vårdgivare eftersom IVO inte vill riskera att påverka verksamheternas rapporteringsvilja. IVO analyserar inte mörkertalet av inrapporterade IT-incidenter, använder dem inte i sina riskanalyser och främjar inte incidentrapporteringen aktivt.

Vårdgivare som omfattas av NIS-lagen ska rapportera in IT-incidenter till MSB som i sin tur delger IVO rapporterna. IVO ska kontrollera att incidentrapporterna följer gällande bestämmelser för vilka incidenter som ska rapporteras in och vid behov begära kompletteringar från verksamheterna. Om en incident gäller hantering av personuppgifter ska IVO rapportera den vidare till IMY.[388]

IVO inleder sällan ett tillsynsärende baserat på incidentrapporteringen. Mellan 2019 och 2023 inledde IVO sex tillsynsärenden på grund av någon form av incident som kommit till IVO:s kännedom, det vill säga inte bara IT-incidenter som rapporterats in enligt NIS-lagen.[389] IVO:s handläggning av IT-incidenter går framför allt ut på att se till att flödet av ärenden fungerar. En anledning till att IVO inte inleder fler tillsynsärenden på grund av incidentrapporter är att myndigheten anser att det kan

386 30 dagar enligt Tillsynsplan NIS 2023.

387 Intervju med företrädare för IVO, 2023-04-20.

388 IVO, *Processbeskrivning, delprocess 3.1.8, rapportering av incident i nätverk och informationssystem*, 2021-10-01.

389 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20. IVO har inte kunnat redovisa vilka av dessa ärenden som öppnats på grund av en inrapporterad IT-incident enligt NIS-lagen eller annan incident som kommit till IVO:s kännedom. Se även IVO:s svar på skriftliga frågor, 2023-12-20.

påverka vårdgivarnas rapporteringsvilja negativt.[390] Detta lyfts även fram i en utvärdering av implementeringen av NIS-lagen som MSB genomfört.[391]

I MSB:s utvärdering av NIS-lagens implementering framkommer att tillsynsmyndigheterna bedömer att bara ett fåtal incidenter rapporteras in. Tänkbara förklaringar är att det inte finns tydligt incitament för en verksamhet att rapportera IT-incidenter, och att MSB:s incidentrapporteringsföreskrift inte är tillräcklig konkret och att det är svårt att tolka vilka incidenter som ska inrapporteras.[392]

Företrädare för IVO gör en liknande bedömning. IVO har identifierat ett antal så kallade vita fläckar av verksamheter som inte inkommer med incidentrapporter, trots att det finns skäl att tro att de borde göra det. Ett exempel är där flera regioner delar samma IT-system, och en region rapporterat in incidenter medan de andra inte gjort det. IVO genomför dock inte systematiska mörkertalsanalyser av vilka vårdgivare som inte rapporterar in incidenter som underlag för sin riskbaserade tillsyn.[393] IVO har inte heller främjat rapporteringsviljan genom riktad information om skyldigheten att rapportera in incidenter till de vårdgivare som sällan eller aldrig gjort det.[394]

4.2.6 IVO saknar kunskap om enskilda vårdgivare och uppmanar inte vårdgivare att anmäla förändringar

IVO tar i sin tillsyn av vårdgivares skyldighet att anmäla sig som leverantör av samhällsviktig tjänst enligt NIS-lagen fram uppgifter om vilka verksamheter som borde kunna vara NIS-leverantörer. Om en potentiell leverantör inte har anmält sig kan IVO inleda en anmälningstillsyn i syfte att avgöra om den bör anmäla sig som leverantör.[395] Mellan 2019 och 2021 fattade IVO beslut i 75 anmälningstillsynsärenden varav 73 gällde kommuner, 1 ärende gällde en region och 1 gällde en enskild vårdgivare. Anledningen till att fler ärenden inte omfattar enskilda vårdgivare är enligt IVO att de inte kunnat få fram tillförlitliga data ur tillgängliga register som möjliggjort tillsyn av enskilda vårdgivare. Det är också anledningen till att IVO inte inledde några anmälningstillsynsärenden under 2022 och 2023.[396]

IVO för register över de vårdgivare som är anmälda som leverantörer av samhällsviktig tjänst, vilket innehåller drygt 200 vårdgivare, och rapporterar

---

390 Intervju med företrädare för IVO, 2023-04-20 och IVO:s svar på skriftliga frågor, 2023-10-04.

391 MSB, *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet, slutrapport,* 2022.

392 MSB, *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet, slutrapport,* 2022.

393 Intervju med företrädare för IVO, 2023-04-20.

394 IVO:s svar på skriftliga frågor, 2023-10-04.

395 Intervju med företrädare för IVO, 2023-04-20. IVO utgår i sin tillsyn av skyldigheten att anmäla sig som leverantör av samhällsviktig tjänst från NIS-lagen och MSB:s föreskrift MSBFS 2021:9. Föreskriften anger vilka krav som ställs på verksamheterna när det gäller att anmäla sig som leverantör, exempelvis vilket ansvar leverantören har för att anmäla förändringar i sin organisation. Grundkravet för att kvalificera sig som leverantör är att man ska ha 50 årsanställda, legitimerad sjukvårdspersonal eller expediera 20 000 medicindoser per år. Alla regioner och de flesta kommuner omfattas därmed, liksom enskilda vårdgivare och apotek. IVO har i sin tillsyn av kommuner satt en undre gräns på 15 000 invånare eftersom det annars blir för få personer som omfattas.

396 IVO:s svar på skriftliga frågor, 2023-12-20.

uppgifterna vidare till MSB.[397] IVO uppger att de har en relativt god överblick över regionala och kommunala vårdgivare men inte om enskilda vårdgivare som de har i sitt register. Anmälda leverantörer är skyldiga att göra ändringsanmälningar till IVO som uppdaterar registret. IVO informerar på sin webbplats om hur uppdateringar av anmälan ska ske men har hittills inte arbetat systematiskt med att proaktivt kontakta leverantörer med information och uppmaningar om att inkomma med ändringar.[398]

4.2.7 IVO ger i liten utsträckning vägledning i tillsynen

IVO ger inte specifika råd om åtgärder till vårdgivare inom ramen för NIS-tillsynen. IVO måste i uppdraget hantera balansen mellan att ge råd och att bedriva tillsyn, och möjligheten till vägledning begränsas av att tillsynen bedrivs som skrivbordstillsyn. IVO menar samtidigt att potentialen för vägledning är störst i enskilda tillsynsärenden.

IVO ska inom ramen för tillsynen ge allmän vägledning vid tillämpningen av NIS-lagen.[399] IVO uppger att man som tillsynsmyndighet har ett övergripande uppdrag att återkoppla iakttagelser och ge råd och vägledning samt sprida information om informationssäkerhet, exempelvis genom att delta i konferenser, men deltagandet styrs av att IVO har begränsat med resurser.[400] Vårdgivare kan också höra av sig till IVO med frågor. Däremot menar IVO att mer konkreta stödinsatser till verksamheterna faller utanför uppdraget.[401]

Samtidigt uppger IVO att det framför allt är i enskilda tillsynsärenden som IVO kan bidra med vägledning och lärande till vårdgivarnas informationssäkerhetsarbete. Tillsynen har särskild potential att bidra till lärande när den sker på plats och hos verksamheter som har lägre kunskaper om informationssäkerhetsarbete. När tillsynen är avslutad uppstår ofta frågor och diskussioner, och när verksamheternas kunskaper är låga kan diskussionerna göra stor skillnad.[402] Detta har framkommit också i vår intervju med en kommun som anser att dialog med IVO i samband med tillsyn varit utvecklande för deras lärande.[403] Men det är enligt IVO en svår balansgång i uppdraget mellan att ge råd och att bedriva tillsyn. Möjligheten att ge konkreta råd som gäller en specifik verksamhet är därför enligt IVO begränsad.[404]

Vägledningen begränsas också av att tillsynen vanligtvis utförs som så kallad skrivbordstillsyn. Eftersom IVO inte anser sig kunna bedriva tillsyn av säkerheten i informationssystemen och nätverken (se avsnitt 4.2.2) begär IVO in och bedömer dokumentation från verksamheten som grund för sina tillsynsbeslut utan att besöka

397 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20. IVO ska rapportera vidare dessa uppgifter utan dröjsmål enligt 19 § 1 st. NIS-förordningen.
398 IVO:s svar på skriftliga frågor, 2023-10-04.
399 19 § NIS-förordningen.
400 Intervju med företrädare för IVO, 2023-04-20.
401 IVO:s svar på skriftliga frågor, 2023-10-04.
402 Intervju med företrädare för IVO, 2023-04-20 och IVO:s svar på skriftliga frågor, 2023-10-04.
403 Intervju med företrädare för kommun 4.
404 Intervju med företrädare för IVO, 2023-04-20 och IVO:s svar på skriftliga frågor, 2023-10-04.

verksamheten och granska deras IT-system. Det minskar möjligheten att ge vägledning och stöd inom ramen för enskilda tillsynsärenden. Enligt företrädare för SKR kan tillsyn från en statlig myndighet öka verksamhetsledningens fokus och ge informationssäkerhetsarbetet en knuff framåt i verksamheten.[405] Eftersom IVO bedriver tillsyn skriftligen och granskar främst om verksamheten har genomfört riskanalyser och tagit fram åtgärdsplaner minskar tillsynens vägledande funktion. Enligt en kommun som varit föremål för tillsyn upplevs tillsynen vara på en generell nivå. Det är inte heller alltid tydligt vad IVO vill att exempelvis en riskanalys ska innehålla. En annan synpunkt är att det krävs en stor insats för att ta fram den information som IVO efterfrågar.[406]

4.2.8 IVO har inte följt upp resultaten av sin tillsyn före 2023

IVO har inte genomfört systematiska uppföljningar av sin tillsyn enligt NIS-lagen före 2023. Det gör att IVO och därmed regeringen saknar kunskap om resultatet av tillsynen, exempelvis att tillsynen begränsats till verksamheters riskanalyser och åtgärdsplaner samt hur sanktionsavgifter påverkar verksamheters informationssäkerhet. IVO har inte heller spridit erfarenheter av tillsynen.

Först under 2023 började IVO följa upp enskilda tillsynsbeslut som innebär att en vårdgivare ska vidta åtgärder för att hantera identifierade bristerna i riskanalyser och åtgärdsplaner. Enligt IVO har myndigheten inte följt upp tillsynsbeslut före 2023 eftersom det tar lång tid för en vårdgivare som ålagts sanktioner att åtgärda de identifierade bristerna i besluten.[407] Ett annat skäl enligt IVO är att det inte funnits tillräckligt många tillsynsärenden att följa upp för att motivera en uppföljning.[408]

IVO ska ta ut sanktionsavgifter av en verksamhet som inte anmäler sig som leverantör av samhällsviktig tjänst, inte vidtar säkerhetsåtgärder för att skydda information eller inte rapporterar IT-incidenter enligt NIS-lagens krav, men IVO kan efterge hela eller delar av avgiften. Avgiften ska vara lägst 5 000 och högst 10 000 000 kronor.[409] Lagstiftningen ger enligt IVO inte någon tydlig vägledning för avgifternas storlek, och det har ännu inte utvecklats en tydlig praxis av att beslut har överklagats och avgjorts i allmän förvaltningsdomstol. IVO har tagit fram en modell för att beräkna sanktionsbeloppen utifrån kriterierna i NIS-lagen.

Mellan 2019 och 2023 utfärdade IVO åtta sanktionsbeslut på grund av att kraven i NIS-lagen inte hade uppfyllts, varav sju gällde kommuner och ett en region. IVO utfärdade därmed avgifter i 10 procent av alla avslutade ärende. Den genomsnittliga

405 Intervju med företrädare för SKR, 2023-06-08

406 Intervju med företrädare för kommun 1.

407 IVO:s svar på skriftliga frågor, 2023-12-20.

408 Intervju med företrädare för IVO, 2023-04-20.

409 Se 29–37 §§ NIS-lagen. Avgiftens storlek ska baseras på den skada som uppstått, om leverantören tidigare har begått en överträdelse, och de kostnader som leverantören har undvikit till följd av överträdelsen. När det gäller anmälningssanktioner och incidentsanktioner är beloppen lägre, medan överträdelser enligt 12 § NIS-lagen om det systematiska informationssäkerhetsarbetet ger högre avgifter enligt modellen.

sanktionsavgiften var knappt en miljon kronor.[410] Under samma period utfärdade IVO 24 sanktionsavgifter som gällde anmälan som leverantör av samhällsviktig tjänst, vilket motsvarar 32 procent av alla ärenden. Ett beslut gällde en enskild vårdgivare, och resten kommuner. Den genomsnittliga sanktionsavgiften var drygt 13 000 kronor.[411] IVO har inte utfärdat sanktionsavgifter på grund av att vårdgivare inte rapporterat in IT-incidenter eller inte gjort det i tid.[412]

IVO har inte utvärderat sin modell för sanktionsavgifterna eller följt upp hur avgifternas storlek påverkar informationssäkerhetsarbetet i berörda verksamheter.

IVO ska årligen lämna en särskild rapport till regeringen med en sammanfattande analys av tillsynsarbetet och de viktigaste iakttagelserna och åtgärder som myndigheten vidtagit med anledning av brister och slutsatser av tillsynen.[413] Erfarenheter av NIS-tillsynen har redovisats i denna rapport vid ett tillfälle, 2020. IVO:s iakttagelser från NIS-tillsynen har därmed sällan presenterats för en bredare krets. IVO har inte heller gjort andra sammanställningar av NIS-tillsynen som spridits till vårdgivare eller till andra myndigheter.[414]

4.3 Gränsdragningsproblematik mellan IMY och IVO

IVO och IMY har närliggande tillsynsuppdrag och det finns en viss gränsdragningsproblematik i tillsynen när det gäller informationssäkerhet för personuppgifter.

IMY:s tillsyn berör skyddet av personuppgifter och utgår från dataskyddsförordningen och kompletterande lagstiftning såsom PDL. IVO:s tillsyn utgår från NIS-lagen och fokuserar på kontinuitet och tillgänglighet i IT-system men omfattar även riktighet, det vill säga skydd av personuppgifter. IVO kan liksom IMY också utgå från PDL i tillsynen. Såväl IVO:s som IMY:s tillsyn omfattar verksamheters tekniska säkerhetsåtgärder för informationssäkerhet i IT-systemen.

Det är framför allt i patientsäkerhetsfrågor inom vården som ansvarsfördelningen mellan myndigheternas tillsyn kan bli otydlig. PDL gäller både vårdgivares behandling av personuppgifter inom vården (IMY:s tillsynsansvar) och skyldigheter att föra patientjournal (IVO:s tillsynsansvar). Gränsdragningsproblemen kan till exempel gälla hur vårdgivarna följer regler som rör journalföring och behandling av

410 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20. Lägsta avgift var 300 000 kronor och högsta 1,7 miljoner kronor.

411 Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20. Lägsta avgift var 5 000 kronor och högsta 45 000 kronor.

412 IVO:s svar på skriftliga frågor, 2023-12-20.

413 3 § förordningen med instruktion för Inspektionen för vård och omsorg.

414 Intervju med företrädare för IVO, 2023-04-20.

personuppgifter, till exempel i behörighetsfrågor.[415] Det kan försvåra för verksamheter att veta till vilken myndighet de ska vända sig till med frågor.[416]

Överlappningarna i uppdragen gör att det finns ett behov av samordning av tillsynen och IMY och IVO slutit en samverkansöverenskommelse och har löpande kontakter. Överenskommelsen har inte utvärderats.[417] I granskningen framkommer viss kritik mot utfallet av samordningen. Enligt SKR har det hänt att IVO:s och IMY:s tillsynsärenden omfattat samma uppgifter och arbete i verksamheterna, till exempel riskanalyser. Enligt SKR saknas det samsyn mellan myndigheterna om hur till exempel en riskanalys bör se ut, men en sådan samsyn skulle underlätta kommuners och regioners arbete.[418] Det är dock enligt IVO inte möjligt att acceptera riskanalyser som IMY bedömt som tillräckliga enligt en annan lagstiftning. Myndigheterna har också delvis olika metodansatser, och det är enligt IVO därför svårt att hitta ett gemensamt sätt att bedöma riskanalyser i tillsynen.[419]

415 IMY:s svar på skriftliga frågor, 2023-10-04 och intervju med företrädare för IVO, 2023-04-20.
416 IMY:s svar på skriftliga frågor, 2023-10-04.
417 IMY:s svar på skriftliga frågor, 2023-10-04. Intervju med företrädare för IVO, 2023-04-20.
418 Intervju med företrädare för SKR, 2023-06-08.
419 IVO:s svar på skriftliga frågor, 2023-10-04.

5 Slutsatser och rekommendationer

Riksrevisionens övergripande slutsats är att statens arbete med att stärka skyddet av personuppgifter som hanteras digitalt inom vården och omsorgen inte är effektivt.

Granskningen visar att MSB:s, IMY:s och Socialstyrelsens styrning och stöd sammantaget inte bidrar effektivt till att stärka vårdens och omsorgens informationssäkerhetsarbete och därmed höja deras informationssäkerhetsnivå. Stödet är generellt och bidrar främst till att vägleda vård- och omsorgsgivare när de ska bygga upp ett informationssäkerhetsarbete i sina verksamheter. Men stödet är inte tillräckligt anpassat efter vård- och omsorgsgivarnas behov, till exempel när det gäller att identifiera och vidta lämpliga organisatoriska och tekniska säkerhetsåtgärder för att hantera risker vid personuppgiftsbehandling och uppnå ett tillräckligt skydd i enlighet med författningsreglerade krav. Vård- och omsorgsgivare ansvarar för informationssäkerheten för personuppgifter men får inte den rättsliga vägledning som de behöver för att kunna tolka författningsreglerade krav. Framför allt mindre kommuner, som har begränsade resurser och brist på den kompetens som krävs, har svårt att fastställa och vidta tillräckliga säkerhetsåtgärder i sitt informationssäkerhetsarbete. MSB, Socialstyrelsen, IMY och IVO har i stor utsträckning valt att inte göra rättsliga ställningstaganden, det vill säga vad de författningsreglerade kraven innebär i praktiken. Det har lett till begränsat rättspraxis och stöd till vård- och omsorgsgivare som behöver göra dessa tolkningar i det praktiska informationssäkerhetsarbetet. Det kan leda till att de inte åtgärdar säkerhetsbrister eller inte fattar beslut om säkerhetsåtgärder, vilket resulterar i ett otillräckligt skydd för personuppgifter. Det riskerar också att leda till att vård- och omsorgsgivare fattar olika beslut om hur samma känsliga personuppgifter ska skyddas, vilket kan leda till varierande skydd för personuppgifter beroende på var i landet man bor. Granskningen visar vidare att myndigheternas samordning av stödet har brister, vilket gjort att statens arbete sammantaget inte bidrar i tillräcklig utsträckning till att stärka skyddet av personuppgifter i vården och omsorgen. Sammantaget är detta enligt Riksrevisionens bedömning inte ett effektivt utnyttjande av samhällets resurser.

Granskningen visar också att tillsynen av vård- och omsorgsgivare inte på ett effektivt sätt kontrollerar om de uppfyller författningsreglerade krav på informationssäkerhet och därigenom nivån för informationssäkerhet. IMY och IVO har genomfört få tillsynsärenden av vårdgivare och inga alls av omsorgsgivare, och tillsynen har sällan omfattat alla delar av verksamheternas informationssäkerhet. Myndigheterna brister också i sitt arbete med att utveckla praxis och ge vägledning inom ramen för tillsynen. Det gör att vård- och omsorgsgivare inte får tillräckligt med vägledning i hur de kan förbättra sitt informationssäkerhetsarbete. Tillsynen är också bara delvis riskbaserad, vilket gör att det är svårt att bedöma om den fokuserar på verksamheter där den skulle ge störst nytta. IMY och IVO har inte heller följt upp sina tillsynsbeslut, vilket

innebär att det är oklart om de granskade verksamheterna har åtgärdat de brister som identifierats vid tillsynen.

Regeringen har genom sin styrning och uppföljning inte sett till att IMY, MSB och Socialstyrelsen har samordnat sitt arbete med att utforma ett stöd som motsvarar vårdens och omsorgens behov på ett effektivt sätt. Regeringen har inte verkat tillräckligt för att socialtjänsten ska omfattas av samma krav på informationssäkerhet som vården, trots att de hanterar liknande känsliga personuppgifter och konsekvenserna därmed är lika stora om uppgifter röjs. Dessutom saknas uttryckliga rättsliga krav på omsorgsgivare och på mindre vårdgivare att arbeta systematiskt med informationssäkerhet, förutom när det gäller behörighetstilldelning och kontroll av dessa behörigheter. Det begränsar bland annat IMY:s och IVO:s möjligheter att bedriva tillsyn av verksamheternas informationssäkerhet.

5.1 Staten arbetar inte effektivt för att stärka regioners och kommuners informationssäkerhetsarbete

Konsekvenserna av att känsliga personuppgifter röjs kan bli stora, både för verksamheter och inte minst för enskilda som drabbas. Flera undersökningar visar att regionernas och framför allt kommunernas informationssäkerhetsarbete har brister och att kommunerna saknar den kompetens och de resurser som krävs för att upprätthålla en väl avvägd nivå på sin informationssäkerhet. Statens samlade arbete bör verka för och stödja vård- och omsorgsgivares informationssäkerhetsarbete så att det leder till ett tillräckligt skydd för information. Riksrevisionens granskning visar att de statliga insatserna i flera avseenden inte är effektiva. Det beror bland annat på att stödet inte är tillräckligt anpassat efter regioners och kommuners behov. Det leder till att regioner och framför allt kommuner upplever osäkerhet i hur bestämmelser för informationssäkerhet ska tolkas när de ska vidta säkerhetsåtgärder för att skydda personuppgifter.

5.1.1 Statens stöd är inte tillräckligt anpassat efter vårdens och omsorgens behov

MSB:s, IMY:s och Socialstyrelsens stöd för informationssäkerhetsarbete är utformat på en övergripande nivå. Riksrevisionen konstaterar att stödet främst är inriktat på hur ett systematiskt informationssäkerhetsarbete ska byggas upp och bedrivas i en verksamhet, oavsett verksamhetsområde och storlek på verksamheten. Myndigheterna ger inte stöd som är tillräckligt anpassat efter vårdens och omsorgens behov, framför allt i komplicerade frågor som berör säkerhetsåtgärder och i avvägningar mellan informationssäkerhet, integritet och patientsäkerhet som kräver hjälp med tolkning av lagstiftningen. Myndigheternas insatser har inte tillräckligt riktats mot de områden där kommuner och regioner anser att de främst behöver stöd, vilket innebär att statens arbete sammantaget inte bidrar till att stärka vårdens och omsorgens informationssäkerhetsarbete.

Rättsliga bestämmelser på området är omfattande och komplexa. Regioner och framför allt kommuner är ofta osäkra på hur bestämmelserna för informationssäkerhet ska tolkas i det praktiska informationssäkerhetsarbetet. Det kan exempelvis handla om lagring av personuppgifter utomlands och i molntjänster, vägledning om vad som är en lämplig miniminivå för organisatoriska och tekniska säkerhetsåtgärder, och stöd för kravställning vid upphandlingar av system som involverar informationssäkerhet. Vård- och omsorgsgivare har behov av rättslig vägledning när de ska fatta beslut om vilka säkerhetsåtgärder som krävs för att skydda personuppgifter i enlighet med författningsreglerade krav. Granskningen visar att myndigheterna sällan ger sådan rättslig vägledning eftersom de är återhållsamma när det gäller tolkning av lagstiftningen. Det är inte heller tydligt för myndigheterna om de faktiskt har i uppdrag att ge sådant stöd till vården och omsorgen.

Brist på rättslig vägledning från myndigheterna leder till att landets regioner och kommuner lägger tid och resurser på att tolka olika bestämmelser, och att det finns risk för att de fattar olika beslut. Enligt Riksrevisionen är det inte resurseffektivt och kan leda till varierande informationssäkerhet över landet, vilket ökar risken för att vissa vård- och omsorgsgivare kan ha otillräcklig nivå på informationssäkerheten.[420] Det är framför allt mindre kommunala vård- och omsorgsgivare som inte har den kompetens och de resurser som krävs. Tydligare rättslig vägledning skulle underlätta för dem att fatta beslut om säkerhetsåtgärder i informationssäkerhetsarbetet för att därigenom uppnå tillräcklig och mer enhetlig informationssäkerhet för personuppgifter.

Granskningen visar dessutom att MSB:s och IMY:s stöd vid inträffade IT-incidenter är begränsat. Vård- och omsorgsgivare som drabbas av exempelvis cyberangrepp får sällan operativt stöd från MSB för att lindra effekterna av det inträffade.

5.1.2 Myndigheterna behöver driva fram praxis

Viktiga förklaringar till att myndigheterna har svårt att ge specifikt stöd är bristen på rättspraxis på såväl nationell nivå som EU-nivå, och deras inställning till att tolka bestämmelserna. IMY är onödigt försiktiga med att tolka dataskyddsförordningen och gör sällan de ställningstaganden i rättsliga frågor som krävs för att driva fram praxis och därigenom specifikt stöd. Det beror på att IMY anser att de måste samarbeta med dataskyddsmyndigheter i andra länder för att få fram gemensam vägledning och praxis. Socialstyrelsen och MSB bidrar inte med rättsligt stöd i enskilda fall för att kunna förklara vad kraven i olika bestämmelser inom vården och omsorgen innebär i praktiken och hur vård- och omsorgsgivare kan förbättra sitt informationssäkerhetsarbete. Som skäl lyfter Socialstyrelsen att det finns en risk med

[420] Som regeringen konstaterar är det i allmänhet dock inte lämpligt att tillsynsmyndigheten uppträder som konsult och ger råd om hur tillsynsobjekten ska agera i specifika ärenden. Det kan till exempel uppstå svårigheter om tillsynsmyndigheten tidigare lämnat mycket precisa råd i ärenden som sedan blir föremål för tillsyn. Tillsynsmyndigheten måste dock självklart kunna lämna upplysningar om vad som utgör gällande rätt (skr. 2009/10:79 s. 17).

att tolka bestämmelserna och ge stöd som inte håller i domstol. Riksrevisionens bedömning är att myndigheterna behöver anpassa sitt arbete med att skapa praxis och specifikt stöd för att motsvara den verklighet som regioner och kommuner står inför. Det är enligt Riksrevisionens bedömning först när de rättsliga förutsättningarna finns på plats som det systematiska informationssäkerhetsarbetet kan bedrivas effektivt inom vården och omsorgen.

5.1.3 Ingen av myndigheterna anser sig ha i ansvar att utforma stödet efter vårdens och omsorgens behov

Ansvaret för att stödja regioners och kommuners informationssäkerhetsarbete är delat mellan MSB, IMY och Socialstyrelsen. Granskningen visar att ingen av myndigheterna anser sig ha tydligt ansvar för och i uppdrag att utforma stöd för informationssäkerhetsarbete efter vårdens och omsorgens behov. Det kan minska effektiviteten i arbetet eftersom ingen tar ansvaret för att tillgodose vårdens och omsorgens behov av specifikt stöd. IMY ska ge stöd till alla sektorer i hur dataskyddsregelverket ska tolkas när personuppgifter behandlas. MSB saknar kompetens och kunskap om vårdens och omsorgens verksamheter och anser inte att de har i uppdrag att ge sektorsspecifikt stöd. MSB anser att det är Socialstyrelsen som har kunskapen om verksamheterna och ansvaret för att meddela föreskrifter, och som därmed ska ge specifikt stöd för vårdens och omsorgens informationssäkerhetsarbete. Socialstyrelsen är sektorsmyndighet för vården och omsorgen, och har meddelat föreskrifter om journalföring och behandling av personuppgifter i vården. Socialstyrelsen har god insyn i och kunskap om vård- och omsorgsgivarnas verksamheter men saknar kompetens inom informationssäkerhet, och anser inte att de har ett tydligt uppdrag att ge specifikt stöd till vårdens och omsorgens informationssäkerhetsarbete. Ingen av de kommuner och regioner som vi har talat med uppfattar heller att de kan få specifikt stöd som berör informationssäkerhet från Socialstyrelsen.

Riksrevisionen bedömer att regeringen behöver göra det tydligt att Socialstyrelsen är den myndighet som ska ansvara för att ge vård- och omsorgsgivare specifikt stöd som berör informationssäkerhet. Socialstyrelsen styr, stödjer och utvecklar verksamheter inom vården och socialtjänsten. I det ingår bland annat att stödja vård- och omsorgsgivarnas arbete med journalföring och behandling av personuppgifter som informationssäkerhet är en viktig del av. Det är enligt Riksrevisionens bedömning därför lämpligt att Socialstyrelsen ska ge anpassat stöd till vårdens och omsorgens informationssäkerhetsarbete.

5.1.4 Myndigheterna arbetar i stuprör och följer inte upp behoven av stöd

Statens samlade insatser bör leda till att stärka vård- och omsorgsgivares informationssäkerhet. Riksrevisionen konstaterar att MSB, Socialstyrelsen och IMY arbetar i stuprör och samverkar inte när de tar fram stödet till samhällets

informationssäkerhet. Konsekvensen blir att det samlade stödet inte är samordnat eller anpassat efter de behov som finns inom vården och omsorgen.

Riksrevisionen konstaterar att myndigheterna sällan använder andra myndigheters uppföljningar och rapporter med information om brister och förbättringsbehov i regioners och kommuners informationssäkerhetsarbete när de tar fram och utvecklar stöd. Det innebär att de går miste om kunskap om brister som finns, vilket ökar risken att stödet inte är anpassat efter alla problemen.

Varken IMY eller Socialstyrelsen följer upp vilka behov av stöd som vården och omsorgen har eller hur det egna stödet tillgodoser deras behov. Därmed saknar de information för att bedöma om de egna stödjande insatserna har bidragit effektivt till att stärka deras informationssäkerhetsarbete. MSB har vid flera tillfällen följt upp det egna stödet och efterfrågat regioners och kommuners behov av stöd. Men MSB har inte anpassat det egna stödet utifrån resultaten så långt som till att ge specifik vägledning till vård och omsorg eftersom man inte anser sig ha ett sådant uppdrag.

Regeringen behöver säkerställa att myndigheterna vid behov samarbetar för att ta vara på varandras kunskaper och kompetenser, så att de kan utforma och anpassa stödet efter vårdens och omsorgens behov.

5.2 Rättsliga bestämmelser om systematiskt informationssäkerhetsarbete omfattar inte omsorgen och mindre vårdgivare

Lagstiftningen ger inte omsorgsgivare samma skyldigheter att skydda personuppgifter som de vårdgivare som omfattas av NIS-lagen, trots att de ofta hanterar lika känsliga uppgifter. Det är särskilt viktigt eftersom regeringen tagit flera initiativ för att underlätta för vård- och omsorgsgivare att samordna olika system för att dela personuppgifter.

Dataskyddsförordningen innehåller generella och tvingande bestämmelser för alla verksamheters skydd av personuppgifter vid behandling. PDL och Socialstyrelsens föreskrifter om journalföring och behandling av personuppgifter preciserar närmare kraven på vårdgivares informationssäkerhet. Motsvarande förtydliganden och krav finns till viss del för socialtjänsten, vilket innebär att det inte ställs samma tydliga krav på omsorgsgivarnas arbete med informationssäkerhet för personuppgifter. Det nya kravet som trädde i kraft i mars 2024, att även omsorgsgivare ska arbeta systematiskt med behörighetstilldelning och kontroll av sådana behörigheter är ett steg i rätt riktning, men otillräckligt. En konsekvens av detta är att kraven för att skydda personuppgifter inte har varit lika tydliga för omsorgsgivare.

Riksdagen och regeringen har bedömt att samhällets aktörer behöver arbeta systematiskt och riskbaserat för att höja sin informationssäkerhetsnivå. Men NIS-lagen och MSB:s föreskrifter om informationssäkerhet ställer enbart krav på vården

att arbeta systematiskt och riskbaserat med informationssäkerhet. Det finns inga motsvarande krav på omsorgsgivare och mindre vårdgivare som inte omfattas av NIS-lagen. Ett problem med detta är att det kan leda till lägre prioritet och bristande engagemang hos regionernas och kommunernas ledningar när det gäller omsorgsgivares och mindre vårdgivares informationssäkerhetsarbete. Ett systematiskt informationssäkerhetsarbete som är välavvägt och anpassat efter verksamhetens behov kan leda till ett kostnadseffektivt skydd och till att säkerhetsincidenter undviks.

5.3 Tillsynen bidrar inte effektivt till att stärka informationssäkerheten

En effektiv tillsyn är viktig för att kontrollera om vård- och omsorgsgivares nivån för informationssäkerhet och efterlevnad av författningsreglerade krav. Tillsyn bidrar också till att ge vägledning till vård- och omsorgsgivare i att göra rätt. NIS-lagen och dataskyddsförordningen trädde i kraft 2018, vilket innebär skärpta krav på informationssäkerhet. Riksrevisionens granskning visar att IMY:s och IVO:s tillsyn är begränsad, och det är oklart om den inriktas mot verksamheter där den gör störst nytta. Tillsynen ger inte heller tillräckligt med rättslig vägledning om vad kraven på informationssäkerhet innebär i praktiken. Det är också oklart vilka effekter tillsynen har haft. IMY:s och IVO:s tillsyn behöver utvecklas för att i högre grad bidra till att stärka informationssäkerheten i vården och omsorgen.

5.3.1 Bristande kontroll av informationssäkerheten

IMY och IVO har i flera avseenden bedrivit en begränsad tillsyn av informationssäkerhet i vården och omsorgen inom ramen för sina respektive uppdrag vilket lett till bristande kontroll av informationssäkerheten, särskilt i kommunal vård och omsorg. Mellan 2018–2023 har varken IMY eller IVO bedrivit tillsyn av omsorgsgivare, och den tillsyn som har genomförts har omfattat få vårdgivare. IVO har också begränsat sin tillsyn av vårdgivare till att gälla delar av NIS-lagen, vilket gör att IVO inte fullt ut granskar den faktiska säkerheten i vårdgivarnas informationssystem och nätverk.

IMY har genomfört få tillsynsärenden av regionala vårdgivares informationssäkerhet och inga alls av kommunala vård- och omsorgsgivares. De kommunala vård- och omsorgsgivarnas informationssäkerhetsarbete har därmed inte varit föremål för kontroll sedan dataskyddsförordningen trädde i kraft. Eftersom IVO har begränsat sin tillsyn av vårdgivares informationssäkerhet till att enbart gälla NIS-lagen har de inte bedrivit tillsyn av omsorgsgivare eller de mindre vårdgivare som inte omfattas av lagen. IVO har dessutom valt att begränsa sin tillsyn av vårdgivare till enbart de bestämmelser i NIS-lagen som ställer krav på verksamheter att ta fram riskanalyser och åtgärdsplaner. En viktig orsak är att Socialstyrelsen ännu inte tagit fram föreskrifter till lagen, trots att regeringen vid flera tillfällen gett myndigheten i uppdrag att ta fram föreskrifterna. IVO anser att de inte kan bedöma om vårdgivare

har vidtagit ändamålsenliga och proportionella tekniska och organisatoriska säkerhetsåtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem i enlighet med NIS-bestämmelserna.

5.3.2 Svårt att bedöma om tillsynen inriktats mot verksamheter där den gör störst nytta

Det är svårt att bedöma om tillsynen inriktats mot verksamheter där den gör störst nytta. Riksrevisionen bedömer att IMY:s och IVO:s egeninitierade riskbaserade tillsyn kan utvecklas och bli mer effektiv om tillsynsmyndigheterna utvecklar sitt arbete med riskanalyser.

IMY och IVO har prioriterat tillsyn av verksamheter som hanterar stora mängder personuppgifter och där antalet personer som potentiellt kan drabbas av en incident är störst, och inte verksamheter som har störst brister. Det har resulterat i att tillsynen framför allt inriktats mot större regionala vårdgivare. IMY har inte genomfört tillsyn av kommunala vård- och omsorgsgivare, och IVO:s tillsyn har i liten utsträckning omfattat mindre kommunala vårdgivare och enskilda vårdgivare.

Granskningen visar också att IMY och IVO inte i tillräcklig utsträckning tagit hänsyn till alla underlag som berör vårdens eller omsorgens brister i informationssäkerheten i sina riskanalyser. Till exempel finns kunskap från andra myndigheter som visar att det framför allt är kommunernas informationssäkerhetsarbete inom vården och omsorgen som har stora brister. De har inte heller analyserat mörkertalen i incidentrapporteringen från regioner och kommuner eller använt dem som underlag i riskanalysarbetet.

Sammantaget kan det leda till att tillsynen inte inriktas tillräckligt mot verksamheter med störst risker för bristande skydd av personuppgifter.

5.3.3 Tillsynen bidrar inte till rättslig vägledning

IMY:s och IVO:s tillsyn bidrar inte på ett effektivt sätt till att vård- och omsorgsgivare får rättslig vägledning om vad kraven på informationssäkerhet innebär i praktiken. IMY anser inte att de kan ge råd inom ramen för enskilda tillsynsärenden. IVO anser inte att de kan uttolka bestämmelserna i NIS-lagen som berör säkerhetsåtgärder i informationssystem och nätverk och vad de innebär i praktiken eftersom Socialstyrelsen inte tagit fram föreskrifter till lagen. Det har, i kombination med att IMY och IVO totalt fattat få tillsynsbeslut, gjort att tillsynen inte ger vård- och omsorgsgivare vägledning för hur de ska göra för att uppfylla olika bestämmelsers krav på skydd av personuppgifter.

IMY och IVO behöver också bli bättre på att förtydliga och sprida sina tillsynsresultat till en bredare krets än de som är föremål för tillsyn i enskilda ärenden, till exempel genom att sammanställa generella iakttagelser och bedömningar från

tillsynsbesluten. Med en bredare återföring ökar förutsättningarna för att tillsynen ska bidra till lärande och utveckling av informationssäkerhetsarbetet.

5.3.4 Tillsynsmyndigheterna behöver följa upp sina beslut

Riksrevisionens bedömning är att IMY och IVO behöver bli bättre på att följa upp om granskade verksamheter har åtgärdat de brister som identifierats vid tillsynen. Tillsynsmyndigheterna har inte följt upp sina tillsynsbeslut systematiskt. Enligt IMY beror det på att tillsynsbesluten ofta överklagas. IVO har sedan 2023 börjat följa upp en del av sina tidigare tillsynsbeslut men har inte gjort det tidigare. Enligt IVO behöver verksamheterna tid för att genomföra de förbättringsåtgärder som krävts i besluten och att det inte funnits tillräckligt med beslut för att göra en systematisk uppföljning. Ingen av myndigheterna har heller följt upp resultatet av de beslut om sanktionsavgifter som de fattar enligt dataskyddsförordningen och NIS-lagen.

Det innebär att det är oklart i vilken utsträckning granskade verksamheter har åtgärdat de brister och problem som identifierats vid tillsynen, och även vilken effekt eventuella sanktioner har haft. Det gör att varken IMY, IVO eller regeringen har en bra bild av nivån för informationssäkerheten i tillsynade verksamheter. En systematisk uppföljning skulle också bidra till att utvärdera träffsäkerheten i myndigheternas riskanalyser.

5.3.5 IMY:s tillsyn är ineffektiv och tar lång tid att genomföra

Riksrevisionen bedömer att IMY kan effektivisera sin verksamhet, till exempel genom att förtydliga sina tillsynsprocesser och ta fram verksamhetsstöd till personalen. På så sätt kan resurser frigöras till den riskbaserade tillsynen som behöver öka i omfattning.

Granskningen visar att IMY:s tillsyn av vårdgivare mellan 2018 och 2022 var delvis riskbaserad och delvis händelsestyrd. Sedan 2021 har antalet riskbaserade och planerade tillsynsärenden minskat kraftigt. En förklaring är ett krav från EDPB 2021 som har resulterat i att IMY måste utreda samtliga klagomål som kommer in till myndigheten. Det har lett till att IMY i huvudsak genomför tillsyn baserat på klagomål från enskilda, vilket tar resurser från arbetet med att bedriva planerad och riskbaserad tillsyn. Till skillnad från riskbaserad tillsyn är den klagomålsbaserade tillsynen av begränsad omfattning.

En annan viktig förklaring är att IMY:s verksamhet är ineffektiv, vilket resulterat i långa handläggningstider. Den genomsnittliga handläggningstiden har legat högt sedan 2020, och IMY har inte lyckats minska tiden trots att effektiviseringsarbete har pågått i flera år. För mer omfattande tillsynsärenden, såsom riskbaserad och planerad tillsyn, var handläggningstiden i genomsnitt omkring 820 dagar. De långa handläggningstiderna beror delvis på att det saknas praxis att stödja sig mot och att IMY är försiktiga med att tolka lagstiftningen och sällan tar fram rättsliga ställningstaganden för att utveckla praxis. IMY lägger därför mycket tid på interna

diskussioner och rättsutredningar för att förankra beslut i enskilda tillsynsärenden. En ytterligare förklaring till att IMY inte inleder fler tillsynsärenden är att många beslut överklagas, vilket enligt IMY kräver resurser. Även relativt hög personalomsättning och otydlig tillsynsprocess har bidragit till de långa handläggningstiderna. Det finns enligt Riksrevisionens bedömning möjligheter för IMY att effektivisera sin handläggning inom ramen för de yttre förutsättningarna för verksamheten.

5.4 Regeringen har inte sett till att styrningen är sammanhållen

Riksrevisionen bedömer att regeringen inte har tydligt fastställt ansvars- och uppgiftsfördelningen mellan IMY, MSB och Socialstyrelsen när det gäller att utforma stöd som motsvarar vårdgivares och omsorgsgivares behov. Regeringen har inte heller sett till att myndigheterna ska samordna sitt arbete för att effektivt utforma stödet. Regeringen har inte heller i tillräcklig utsträckning följt upp och skapat sig en samlad bild av myndigheternas arbete med stödjande insatser.

Dessutom har regeringen vidtagit få åtgärder för att myndigheternas stöd till vårdens och omsorgens informationssäkerhetsarbete ska bli mer anpassat efter deras behov. Regeringen har visserligen beslutat om statsbidrag för kommuner, slutit överenskommelser med SKR om stödjande insatser, tillsatt flera utredningar som delvis berör frågor om informationssäkerhet. Men dessa åtgärder har inte varit tillräckligt inriktade för att stärka vårdens och omsorgens informationssäkerhet.

Trots att omsorgen ofta hanterar lika känsliga personuppgifter som vården, har regeringen inte verkat tillräckligt för att omsorgsgivare ska omfattas av samma tydliga krav på säkerhetsåtgärder och systematiskt informationssäkerhetsarbete som vårdgivare, förutom när det gäller viss behörighetstilldelning och kontroll av behörigheterna.

5.5 Rekommendationer

Riksrevisionen bedömer att staten behöver arbeta mer effektivt med styrning av, stöd till och tillsyn av vård- och omsorgsgivares informationssäkerhetsarbete. Riksrevisionen lämnar därför nedanstående rekommendationer till regeringen och myndigheter i syfte att stärka vård- och omsorgsgivares informationssäkerhetsarbete.

Till regeringen

- Förtydliga Socialstyrelsens ansvar för att ta fram verksamhetsanpassat stöd till vårdens och omsorgens informationssäkerhetsarbete. Stödet bör utformas utifrån vård- och omsorgsgivares behov och i samråd med relevanta myndigheter. Stödet kan bland annat innebära att:
    - identifiera sektorsspecifika risker och sårbarheter för informationssäkerhet.

    - ge exempel på lämpliga organisatoriska och tekniska säkerhetsåtgärder för informationssäkerhet.
    - ge stöd och vägledning i hur bestämmelserna för skydd av personuppgifter bör tolkas i generella fall.
- Utred hur omsorgsgivare fullt ut kan omfattas av motsvarande bestämmelser för skydd av personuppgifter som vårdgivare.
- Säkerställ att omsorgsgivare och mindre vårdgivare som inte omfattas av NIS-lagen omfattas av krav på att bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Till Inspektionen för vård och omsorg

- Bedriv tillsyn som granskar om vårdgivare faktiskt uppfyller NIS-lagens samtliga krav på säkerhet i nätverk och informationssystem.
- Utveckla arbetet med riskanalyser så att tillsynen i större utsträckning inriktas mot områden där bristerna i informationssäkerhet är som störst.
- Utveckla uppföljningen av tillsynsbeslut för att säkerställa att tillsynen får avsedd effekt.

Till Integritetsskyddsmyndigheten

- Effektivisera handläggningen av klagomåls- och tillsynsärenden och frigör därigenom resurser för att bedriva mer riskbaserad tillsyn.
- Utveckla arbetet med riskanalyser så att tillsynen i större utsträckning inriktas mot områden där bristerna i informationssäkerhet är som störst.
- Utveckla uppföljningen av tillsynsbeslut för att säkerställa att tillsynen får avsedd effekt.

Ordlista

Beröringspunkterna mellan dataskydd, informationssäkerhet och cybersäkerhet är många. I grunden är det ofta samma typ av systematiska arbete och åtgärder som behövs för att förebygga hot mot den personliga integriteten och för att stärka skyddet för samhällets säkerhet.

Cyberangrepp (eller IT-angrepp)
Ett cyberangrepp är ett försök att få obehörig åtkomst till nätverk och informationssystem för att stjäla, ändra, otillgängliggöra eller förstöra data.

Cybersäkerhet
Det finns ingen standardiserad, allmän definition av cybersäkerhet. Europeiska revisionsrätten definierar cybersäkerhet som den verksamhet som krävs för att skydda nätverks- och informationssystem, deras användare och övriga personer som berörs av cyberhot. Det inbegriper förebyggande, detektering och hantering av samt återställning efter cyberincidenter. Dessa incidenter orsakas av händelser som kan vara planerade eller oplanerade och omfatta oavsiktligt röjande av information, angrepp mot företag och kritisk infrastruktur, stöld av personuppgifter och till och med inblandning i demokratiska processer och val. De kan även omfatta allmänna desinformationskampanjer som syftar till att påverka den offentliga debatten.[421] Se även Informationssäkerhet och Dataskydd.

Dataskydd
Dataskydd innebär att var och ens rättigheter och friheter tillgodoses vid behandling av personuppgifter. Syftet med dataskydd är att ange när och under vilka förutsättningar personuppgifter kan behandlas. Se även Informationssäkerhet och Cybersäkerhet.

Informationsklassning
Att klassa sin information avseende konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser ett bristande skydd kan få.[422] Att klassa informationstillgångar innebär att genom konsekvensanalyser identifiera skyddsbehov för information och resurser som hanterar information.

Informationssäkerhet
Bevarande av konfidentialitet, riktighet och tillgänglighet hos information.[423] Informationssäkerhet innefattar både organisatorisk säkerhet och teknisk säkerhet (se vidare Säkerhetsåtgärder). Andra närliggande begrepp som används för att beskriva samma grundläggande systematiska arbete är dataskydd och cybersäkerhet. Beröringspunkterna mellan de olika begreppen är många. I grunden är det ofta

421 Kontaktkommittén för de högre revisionsorganen inom Europeiska unionen (2020), Cybersäkerhet i EU och medlemsstaterna, s. 9.
422 6 § 1 MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
423 3 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

samma typ av säkerhetsåtgärder som behövs för att förebygga hot mot den personliga integriteten och för att stärka skyddet för samhällets säkerhet. I granskningen används begreppet informationssäkerhet.

IT-incident eller informationssäkerhetsincident
En IT-incident är en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem.[424] Informationssäkerhetsincidenter kan samtidigt vara andra typer av incidenter såsom personuppgiftsincidenter.

Konfidentialitet
Konfidentialitet är en egenskap hos en informationstillgång som innebär att den inte tillgängliggörs eller avslöjas för obehöriga individer, objekt eller processer.

Ledningssystem för informationssäkerhet
Del av myndighetens övergripande ledningssystem, baserat på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet.[425] Ledningssystemet omfattar organisationsstruktur, policyer, planeringsaktiviteter, ansvar, praxis, rutiner, processer och resurser.

Omsorgsgivare
Den som ansvarar för eller utför insatser för äldre personer eller personer med funktionsnedsättning.[426]

Patientinformation
Personuppgifter som hanteras i journalsystem, kvalitetsregister och liknande.

Personuppgift
All information som handlar om fysiska personer som kan identifieras är personuppgifter. Det spelar ingen roll om individen är direkt identifierbar genom uppgiften, eller om det krävs ytterligare information för att individen ska kunna identifieras.[427]

Personuppgiftsansvarig
Den organisation, till exempel aktiebolag, stiftelse, förening eller myndighet, som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till.[428]

Personuppgiftsincident
En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller

---

424 2 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
425 3 § MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).
426 Omsorgsgivare definieras i 1 § lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation. I granskningen använder vi begreppet i en allmän mening för verksamheter som bedriver omsorg om äldre och personer med funktionsnedsättning. Se avsnitt 1.2.
427 IMY, ”Introduktion till dataskyddsförordningen”, hämtad 2023-02-13.
428 IMY, ”Personuppgifts-ansvariga och personuppgiftsbiträden”, hämtad 2023-02-13.

olaglig förstöring, förlust eller ändring av personuppgifter. Den kan också leda till ett obehörigt röjande av eller obehörig åtkomst till personuppgifter.[429]

Riktighet
Egenskap hos informationstillgång som innebär att den skyddas mot oönskad förändring.

Säkerhetsåtgärder
För att skydda information krävs säkerhetsåtgärder, det vill säga åtgärder för att möta en organisations risker. Säkerhetsåtgärder för informationssäkerhet omfattar åtgärder inom det organisatoriska, personrelaterade, tekniska och fysiska säkerhetsområdet. Åtgärderna kan verka förebyggande, upptäckande eller korrigerande. Inom det *organisatoriska området* återfinns exempelvis policyer och riktlinjer, interna rutiner och instruktioner, roll- och ansvarsfördelning och ledningens ansvar samt hantering av informationssäkerhetsincidenter. *Personrelaterade åtgärder* inbegriper bland annat bakgrundskontroll samt medvetenhet och utbildning inom informationssäkerhet. *Tekniska säkerhetsåtgärder* avser bland annat åtkomsträttigheter, säkerhetskopiering av information, inloggning, brandväggar, kryptering och antivirusskydd. Med *fysiska säkerhetsåtgärder* avses exempelvis fysiskt skalskydd och tillträde, arbete i säkrade utrymmen och placering och skydd av utrustning.[430]

Tillgänglighet
Innebär i informationssäkerhetssammanhang att en informationstillgång är åtkomlig och användbar inom förväntad tid och i förväntad omfattning.

Vårdgivare
Statlig myndighet, region, kommun, annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvårdsverksamhet.[431]

---

429 IMY, ”Anmäl personuppgifts-incident”, hämtad 2023-02-17.

430 Svenska institutet för standarder, Svensk standard SS-ISO/IEC 27002:2022, *Informationsteknik – Säkerhetstekniker – Riktlinjer för informationssäkerhetsåtgärder (ISO/IEC 27002:2022, IDT)*, utgåva 3.

431 2 kap. 3 § hälso- och sjukvårdslagen (2017:30).

Referenslista

Rapporter, utredningar, interna styrdokument m.m.

Datainspektionen, *Behovs- och riskanalys inom hälso- och sjukvården – en vägledning*, dnr. DI-2020-11495, Datainspektionen 2020.

Datainspektionen, *Tillsynsplan 2019–2020*, dnr. DI-2019-841, IMY 2019-03-22.

EDPB 2021, *Riktlinjer 01/2021 om exempel på anmälan av personuppgiftsincidenter*, Version 2.0, IMY 2021-12-14.

IMY, *Anmälda personuppgiftsincidenter 2021,* IMY 2022.

IMY, *Anmälda personuppgiftsincidenter 2022,* IMY 2023.

IMY, *En uppgift om förvaltarskap enligt 11 kap. föräldrabalken är en känslig personuppgift*, (IMYRS 2022:3), IMY 2022.

IMY, *Integritetsskyddsmyndighetens budgetunderlag 2022–2024*, IMY 2021.

IMY, *Integritetsskyddsmyndighetens budgetunderlag 2024–2026,* IMY 2023.

IMY, *IMY:s mål- och resultatkarta*, IMY 2021.

IMY, *IMY:s policy för tillsyn*, dnr. DI-2021-1697, IMY 2021.

IMY, *Innebörden av begreppet ”personuppgifter som rör lagöverträdelser som innefattar brott” i artikel 10 i dataskydds-förordningen* (IMYRS 2021:1), IMY 2021

IMY, *Klagomål till IMY – den nationella bilden 2021 (2022:2)*, IMY 2022.

IMY, *Projektdirektiv – Utveckla arbetet med anmälda personuppgiftsincidenter*, dnr. IMY-2023-3926, IMY 2023-04-24.

IMY, *Rätten till borttagande av sökträffar avseende publiceringar i nyhetsmedier m.m (*IMYRS 2022:1), IMY 2022.

IMY, *Ställningstagande om partsställning i ärenden som inleds med anledning av klagomål*, IMY 2023.

IMY, *Tillsynsplan 2021–2022*, dnr. DI-2020-1697, IMY 2021-03-04.

IMY, *Tillsynsplan 2023*, IMY-2023-6415, IMY 2023-05-08.

IMY, *Tillsynsplan 2024*, IMY-2024-2859, IMY 2024-03-11.

IMY, *Undantaget för journalistiska ändamål i 1 kap. 7 § andra stycket dataskyddslagen* (IMYRS 2022:2), IMY 2022.

IMY, *Verksamhetsplan för 2023,* IMY 2022.

IMY, *Årsredovisning 2020*, IMY, 2021.

IMY, *Årsredovisning 2021*, IMY 2022.

IMY, *Årsredovisning 2022*, IMY 2023.

IVO, *Processbeskrivning, delprocess 3.1.8, rapportering av incident i nätverk och informationssystem*, dnr. 1.1.2- 45452/2020, IVO 2021-10-01.

IVO, *Tillsynsplan NIS 2020*, IVO 2020.

IVO, *Tillsynsplan NIS 2021*, IVO 2021.

IVO, *Tillsynsplan NIS 2022*, IVO 2022.

IVO, *Tillsynsplan NIS 2023*, IVO 2023.

IVO, *Vad har IVO sett 2017? Iakttagelser och slutsatser om vårdens och omsorgens brister för verksamhetsåret 2017*, IVO 2018.

IVO, *Vad har IVO sett 2018? Iakttagelser och slutsatser om vårdens och omsorgens brister för verksamhetsåret 2018*, IVO 2019.

IVO, *Vad har IVO sett 2019? Iakttagelser och slutsatser om vårdens och omsorgens brister för verksamhetsåret 2019*, IVO 2020.

IVO, *Vad har IVO sett 2020? Iakttagelser och slutsatser om vårdens och omsorgens brister för verksamhetsåret 2020*, IVO 2021.

IVO, *Vad har IVO sett 2021? Iakttagelser och slutsatser om vårdens och omsorgens brister för verksamhetsåret 2021*, IVO 2022.

IVO, *Vad har IVO sett 2022? Iakttagelser och slutsatser om vårdens och omsorgens brister för verksamhetsåret 2022*, IVO 2023.

IVO, *Årsredovisning 2019*, IVO 2020.

IVO, *Årsredovisning 2022*, IVO 2021.

MSB, Behovsanalys informationssäkerhet, upplevda hinder vid systematiskt informationssäkerhetsarbete, MSB 2023.

MSB, *Det systematiska informations- och cybersäkerhetsarbetet i den offentliga förvaltningen, resultatredovisning av Infosäkkollen och It-säkkollen 2023*. MSB 2024.

MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen, resultatredovisning Infosäkkollen 2021*, MSB 2022.

MSB, *En inblick i Sveriges cybersäkerhet: Årsrapport IT-incidentrapportering 2021*, MSB 2022.

MSB, *EU förändrar cybersäkerhetsområdet. Årsrapport IT-incidentrapportering 2023*. MSB 2024.

MSB, *It-incidenter som påverkar samhällsviktiga och digitala tjänster – NIS-leverantörers IT-incidentrapportering 2021,* MSB 2022.

MSB, *Metodstöd för systematiskt Informationssäkerhetsarbete,* MSB 2021.

MSB, *När kriget kom nära. Årsrapport IT-incidentrapportering 2022,* MSB 2023.

MSB, *Uppdrag till Myndigheten för samhällsskydd och beredskap att stärka funktionen CERT-SE samt utveckla och förenkla det stöd som lämnas inom informations- och Cybersäkerhetsområdet - redovisning av regeringsuppdrag Ju2022/02219*, MSB 2023.

MSB, *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet, slutrapport*, MSB 2022.

MSB, *Utvärdering av metodstöd,* MSB 2022.

MSB, *Utvärdering av resultatet av Sveriges implementering av NIS-direktivet*, MSB 2022.

MSB, *Årsredovisning 2022*, MSB 2023.

Myndigheten för vård- och omsorgsanalys, *Digital potential - Utvärdering av satsningen på digital teknik i äldreomsorgen (2023:6)*, Myndigheten för vård- och omsorgsanalys 2023.

Riksrevisionen, Analys av frågor till MSB:s rådgivningstjänst för systematiskt informationssäkerhetsarbete från kommuner och regioner samt MSB:s svar, september 2022 till och med januari 2023. Riksrevisionen 2023.

Riksrevisionen, Analys av ett urval kvalificerade frågor och svar från vård- och omsorgsgivare till IMY 2018–2022. Riksrevisionen 2023.

Riksrevisionen, *Informationssäkerhet vid universitet och högskolor – hanteringen av skyddsvärda forskningsdata (RiR 2023:20)*, Riksrevisionen 2023.

Riksrevisionen, *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig (RiR 2023:8)*, Riksrevisionen 2023.

Riksrevisionens sammanställning och analys av uppgifter från IVO 2023-05-05 och 2023-12-20 om tillsynsärenden enligt NIS-lagen, Riksrevisionen 2023.

Riksrevisionen, *Statens tillsyn över apotek och partihandel med läkemedel (2022:11)*, Riksrevisionen 2022.

SKR, *Kommunernas informationssäkerhetsarbete – En övergripande kartläggning av kommunernas systematiska informationssäkerhetsarbete*, Sveriges Kommuner och Regioner 2019.

Socialstyrelsen, *Journalföring och behandling av personuppgifter i hälso- och sjukvården,* Socialstyrelsen 2017.

Socialstyrelsen, *Säker personuppgiftsbehandling i socialtjänsten. Rättsläge och utgångspunkter*, Socialstyrelsen 2018.

Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2022.*, Socialstyrelsen 2022.

Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2023.*, Socialstyrelsen 2023.

Socialstyrelsen, *Redovisning av 2021 års statsbidrag till kommuner för att säkerställa god vård och omsorg av äldre personer,* Socialstyrelsen 2022.

Socialstyrelsen, *Redovisning av 2022 års statsbidrag till kommuner för att säkerställa god vård och omsorg av äldre personer,* Socialstyrelsen 2023.

Socialstyrelsen, *E-hälsa och välfärdsteknik i kommunerna 2023,* Socialstyrelsen 2023.

Socialstyrelsen, *Årsredovisning 2019,* Socialstyrelsen 2020.

Socialstyrelsen, *Årsredovisning 2020,* Socialstyrelsen 2021.

SOU 2016:65, *Ett samlat ansvar för tillsyn över den personliga integriteten*.

SOU 2017:36, *Informationssäkerhet för samhällsviktiga och digitala tjänster*.

SOU 2015:23, *Informations- och cybersäkerhet i Sverige*.

SOU 2022:6, *Hälso- och sjukvårdens beredskap – struktur för ökad förmåga*.

SOU 2023:83, *Samordnat juridiskt stöd och vägledning för hälso- och sjukvårdens digitalisering*.

SOU 2024:18, *Nya regler om cybersäkerhet. Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven*.

Statskontoret, *Myndighetsanalys av Datainspektionen (2020:14),* Statskontoret 2020.

Statskontoret, *På väg mot en bättre tillsyn? En studie av den statliga tillsynens utveckling*, Statskontoret 2020.

Riksdagstryck och regeringsbeslut

Prop. 2007/08:126, *Patientdatalag m.m,* bet 2007/08:SoU16, rskr. 2007/08:207.

Prop. 2012/13:20, *Inspektionen för vård och omsorg - en ny tillsynsmyndighet för hälso- och sjukvård och socialtjänst*, bet. 2012/13:SoU5, rskr. 2012/13:116.

Prop. 2017/18:205, *Informationssäkerhet för samhällsviktiga och digitala tjänster*, skr. 2016/17:213.

Prop. 2019/20:1, *Budgetpropositionen för 2020,* bet. 2019/20:FiU1.

Prop. 2021/22:177, *Sammanhållen vård- och omsorgsdokumentation*, bet. 2021/22:SoU30, rskr. 2021/22:381.

Prop. 2020/21:1, *Budgetpropositionen för 2021,* bet. 2020/21:FiU2, rskr. 2020/21:150.

Prop. 2022/23:131, *Välfärdsteknik inom äldreomsorgen,* bet. 2023/24:SoU3.

Prop. 2023/24:1, *Budgetpropositionen för 2024,* bet. 2023/24:FiU1.

Regeringsbeslut Ju2018/02265/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att förbättra kommunernas informationssäkerhet i samarbete med länsstyrelserna.*

Regeringsbeslut Ju2019/03057/SSK, *Uppdrag till MSB att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor.*

Regeringsbeslut, Ju2018/03737/SSK, *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.*

Regeringsbeslut Ju2019/03058/SSK, *Uppdrag till MSB att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.*

Regeringsbeslut Ju2019/02421/SSK, *Uppdrag till MSB att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.*

Regeringsbeslut Ju2022/02219, *Uppdrag till Myndigheten för samhällsskydd och beredskap att stärka funktionen CERT-SE samt utveckla och förenkla det stöd som lämnas inom informations- och cybersäkerhetsområdet.*

Regeringsbeslut S2019/04518/FS, *Regleringsbrev för budgetåret 2019 avseende Socialstyrelsen.*

Regeringsbeslut S2020/00574/FS, *En strategi för genomförande av Vision e-hälsa 2025.*

Regeringsbeslut 2020/00577/SOF, *Överenskommelse mellan staten och Sveriges Kommuner och Regioner om äldreomsorg – teknik, kvalitet och effektivitet med den äldre i fokus.*

Regeringsbeslut S2020/09552, *Regleringsbrev för budgetåret 2020 avseende Socialstyrelsen.*

Regeringsbeslut S2021/07588 (delvis) *Regleringsbrev för budgetåret 2021 avseende Socialstyrelsen.*

Regeringsbeslut S2022/04549, *Regleringsbrev för budgetåret 2022 avseende Socialstyrelsen.*

Regeringsbeslut S2023/00374, *Överenskommelse mellan staten och Sveriges Kommuner och Regioner om hälso- och sjukvårdens arbete med civilt försvar 2023.*

Regeringsbeslut S2023/02343, *Regleringsbrev för budgetåret 2023 avseende Socialstyrelsen.*

Skr. 2016/17:213, *Nationell strategi för samhällets informations- och cybersäkerhet*, bet. 2017/18:FöU4, rskr 2017/18:142.

Rättsliga dokument

Domstolsbeslut, Förvaltningsrätten Stockholm, målnummer 4721-22, 2023-11-16.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Europaparlamentets och rådets förordning (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

EU:s dataskyddsdirektiv (95/46/EG).

EU-domstolens dom C-518/07.

Förordning (2001:637) om behandling av personuppgifter inom socialtjänsten.

Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten.

Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

Förordning (2013:176) med instruktion för Inspektionen för vård och omsorg.

Förordning (2015:284) med instruktion för Socialstyrelsen.

Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.

Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Förordning (2022:524) om statliga myndigheters beredskap.

Förvaltningslag (2017:900).

Hälso- och sjukvårdslag (2017:30).

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen).

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Lag (2001:454) om behandling av personuppgifter inom socialtjänsten.

Lag (2022:913) om sammanhållen vård- och omsorgsdokumentation.

Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8).

Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd om rapportering av incidenter för leverantörer av samhällsviktiga tjänster (MSBFS 2018:9).

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2021:9).

Offentlighets- och sekretesslag (2009:400).

Patientdatalag (2008:355).

Patientdataförordningen (2008:360).

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för ett systematiskt kvalitetsarbete (SOSFS 2011:9).

Socialstyrelsens föreskrifter och allmänna råd om vårdgivares systematiska patientsäkerhetsarbete (HSLF-FS 2017:40)

Socialtjänstlag (2001:453).

Webbsidor och tidningsartiklar

Gunnarsson, L., ”Cyberattack mot Ölandskommunerna”, *Kalmarposten*, 2022-12-13, https://www.kalmarposten.se/oland/cyberattack-mot-olandskommunerna/ , hämtad 2022-12-13.

Humana, ”IT-angrepp från tredje part”, https://www.humanagroup.se/media/pressmeddelanden/2023/IT-angrepp-fran-tredje-part/, hämtad 2023-03-07.

IMY, ”Brister i hur vårdgivare styr personalens åtkomst till journaluppgifter”, https://www.imy.se/nyheter/brister-i-hur-vardgivare-styr-personalens-atkomst-till-journaluppgifter/, hämtad 2023-11-15.

IMY, ”Systematisk logguppföljning”, https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/vard/systematisk-logguppfoljning/, hämtad 2023-10-26.

MSB, ”Detta är informationssäkerhet”, https://www.informationssakerhet.se/om-informationssakerhet2/vad-ar-informationssakerhet/, hämtad 2022-11-09.

MSB, ”Metodstöd”, https://www.informationssakerhet.se/metodstodet/, hämtad 2024-02-06.

MSB, ”Rådgivningstjänst för systematiskt informationssäkerhetsarbete”, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/radgivningstjanst-for-systematiskt-informationssakerhetsarbete/, hämtad 2023-05-08.

MSB, ”Termbank för informationssäkerhet”, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/standardisering-inom-informationssakerhet/termbank-for-informationssakerhet/, hämtad 2023-11-11.

SVT Nyheter, ”Miljonkostnader för Kalix kommun efter IT-attacken”, https://www.svt.se/nyheter/lokalt/norrbotten/miljonkostnader-for-kalix-kommun-efter-it-attacken, hämtad 2022-01-14.

Bilaga 1. Rättsliga bestämmelser m.m. rörande informationssäkerhet för personuppgifter och sekretess

I bilagan ges en definition av informationssäkerhet och en översiktlig beskrivning av bestämmelser rörande informationssäkerhet för personuppgifter inom vård och omsorg och om sekretess. Vården och omsorgen ansvarar för all personuppgiftsbehandling. Det är respektive vård- eller omsorggivares ansvar att det finns processer, rutiner och åtgärder som säkerställer att verksamheten uppfyller de krav och mål som ställs i lagar, förordningar och föreskrifter vad gäller informationssäkerhet för personuppgifter. En annan förutsättning för att rättsliga bestämmelser aktualiseras är vanligen att vårdgivare eller omsorgsgivare behandlar personuppgifterna i ett system som är helt eller delvis automatiserat.

Definition av informationssäkerhet

Den internationellt fastslagna definitionen av informationssäkerhet är de åtgärder för bevarande av konfidentialitet, riktighet och tillgänglighet hos information.[432] Dessa egenskaper kompletteras ibland med andra egenskaper såsom spårbarhet och ansvarsskyldighet. Informationssäkerhet omfattar både administrativ säkerhet och teknisk säkerhet.

Administrativ säkerhet är de åtgärder som styr informationssäkerhetsarbetet och handlar om styrdokument, utbildning, rutiner, övervakning av efterlevnad och uppföljning. Administrativ säkerhet delas in i formell och informell säkerhet. Formell säkerhet innebär rutiner för styrning och ledning av informationssäkerhet. Informell säkerhet är medarbetares uppfattningar, värderingar och attityder som påverkar deras agerande i informationssäkerhet.

Teknisk säkerhet är åtgärder som ska skydda informationssystem och nätverk för lagring och delning av personuppgifter. En organisation behöver därför ta ett helhetsgrepp och skapa fungerande processer i organisationen för att skydda informationen på rätt sätt.[433] Ytterst styrs informationssäkerhetsarbetet av ledningen bland annat genom styrning, tilldelning av resurser, beslutsfattande och eget engagemang.

[432] Swedish Standards Institute, Teknisk rapport SIS-TR 50:2015 Terminologi för informationssäkerhet s. 9. Se också Skr. 2016/17:213, s. 4 och Informationssäkerhet.se, ”Detta är informationssäkerhet”, hämtad 2022-09-26.

[433] Swedish Standards Institute, Teknisk rapport SIS-TR 50:2015 Terminologi för informationssäkerhet, s. 9.

Sekretess för offentliga aktörer och förhållandet till dataskyddsregelverket

Offentlighets- och sekretesslagen (2009:400), OSL, innehåller bland annat bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud mot att lämna ut allmänna handlingar. Dessa bestämmelser avser förbud mot att röja uppgift, vare sig detta sker muntligen, genom utlämnande av allmän handling eller på annat sätt (1 kap. 1 § OSL). Sekretess gäller mot enskilda och mot andra myndigheter samt mellan olika självständiga verksamhetsgrenar inom myndigheter (8 kap. 1 och 2 §§ OSL).

Enligt 25 kap. 1 § OSL råder sekretess till skydd för uppgifter om patienter inom den allmänna hälso- och sjukvården. Sekretessen tar i första hand sikte på den hälso- och sjukvård som bedrivs av det allmänna i sjukhus och andra vårdinrättningar. Bestämmelsen omfattar också verksamheten vid inrättningar för öppen vård, distriktsläkarmottagningar, folktandvårdskliniker med flera. Utanför bestämmelsens tillämpningsområde faller däremot verksamhet vid sjukhus och andra liknande inrättningar som drivs av enskilda. Här gäller i stället bestämmelserna om tystnadsplikt med mera i 6 kap. patientsäkerhetslagen (2010:659).

Enligt 26 kap. 1 § OSL råder sekretess till skydd för uppgifter om enskildas personliga förhållanden inom socialtjänsten. Verksamheten behöver inte bestå i handläggning av ett ärende utan kan utgöras av rent faktisk verksamhet. Sekretessen omfattar bland annat handlingar och uppgifter i övrigt som gäller uppsökande verksamhet, social hemhjälp, kontaktverksamhet, vård och behandling vid kommunernas och regionernas institutioner såsom barn- eller ungdomshem, behandlingshem, inackorderingshem och särskilt boende för äldre samt över huvud taget social service och socialt bistånd som lämnas av socialnämnd.

OSL och dataskyddsförordningen är två skilda regelverk. Vad som är tillåtet enligt förordningen är inte alltid tillåtet enligt OSL och vice versa. Riksdagens ombudsmän (JO) har konstaterat det kan vara vanskligt att försöka hitta en gemensam standard för myndigheters hantering av uppgifter.[434] Bedömningen skiljer sig åt mellan regelverken, och bara den omständigheten att det i dataskyddsförordningen ställs upp särskilda regler för hur en viss uppgift får behandlas (till exempel i artikel 9) innebär inte per automatik att uppgiften också omfattas av sekretess enligt OSL. Däremot kan den omständigheten att en uppgift omfattas av sekretess enligt OSL vara en indikation på att det i dataskyddsförordningen uppställs särskilda regler för hur den får behandlas. Enligt JO är det en offentlig vård- eller omsorgsgivares ansvar att i varje enskilt fall säkerställa att en viss uppgift hanteras i enlighet med bestämmelserna i både OSL och dataskyddsförordningen.[435]

---

434 Se JO:s beslut 2020-11-02, dnr 3224–2019.

435 Enligt JO är utgångspunkten dessutom att sekretessen för uppgift om t.ex. patientinformation innebärande ett förbud mot röjande av densamma i regel inte påverkas av att en vårdgivare kan upprätthålla ett tekniskt skydd för uppgifterna, se JO:s beslut 2014-09-09.

Bestämmelser om behandling av personuppgifter inom hälso- och sjukvården och omsorgen

Hälso- och sjukvården och socialtjänsten behandlar stora mängder skyddsvärda personuppgifter om enskildas hälsa, livsstil, familjeförhållanden och ekonomiska förhållanden. Begreppet personuppgifter är brett.[436]

Vid vård av patienter ska det föras patientjournal i syfte att bidra till en god och säker vård av patienten.[437] Den som för patientjournal ansvarar för uppgifter i journalen.[438]

Bestämmelser för informationssäkerhet inom vård och omsorg

Flera lagar, förordningar och föreskrifter ställer krav på informationssäkerhet för personuppgifter hos regioner och kommuner och vård- och omsorgsgivare.[439]

Dataskyddsförordningen gäller för behandling och skydd av personuppgifter

Bestämmelser om skydd av fysiska personers personuppgifter finns i EU:s dataskyddsförordning.[440] Dataskyddsförordningen började att tillämpas den 25 maj 2018 och ett av syftena med dataskyddsförordningen är att skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.[441] Dataskyddsförordningen är direkt tillämplig och har företräde framför nationell lagstiftning.

Den som är personuppgiftsansvarig ansvarar för att behandling av personuppgifter är laglig och följer bestämmelserna i dataskyddsförordningen och ska också kunna visa att detta.[442] Vid behandling av personuppgifter inom hälso- och sjukvården är vårdgivaren personuppgiftsansvarig. I en region och en kommun är varje myndighet som bedriver hälso- och sjukvård personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför.[443] Vid behandling av personuppgifter inom

---

436 Artikel 4.1 i dataskyddsförordningen: Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

437 3 kap. 2 § patientdatalagen.

438 3 kap. 4 § patientdatalagen.

439 Med begreppet vårdgivare avses en statlig myndighet, region eller kommun i fråga om sådan hälso- och sjukvård som myndigheten, regionen eller kommunen har ansvar för (offentlig vårdgivare) samt annan juridisk person eller enskild näringsidkare som bedriver hälso- och sjukvård (privat vårdgivare).

440 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

441 Artikel 1 och 2 i dataskyddsförordningen. Se även artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (EKMR). Skydd för personuppgifter regleras även i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (EU-stadgan).

442 Artiklarna 4.7 och 5.2 i dataskyddsförordningen.

443 2 kap. 6 § patientdatalagen.

omsorgen är den kommunala myndigheten eller den enskilda verksamhet som bedriver omsorgen personuppgiftsansvarig.[444] Även personuppgiftsbiträden har skyldigheter i dataskyddsförordningen.[445]

Dataskyddsförordningen utgår från ett antal grundläggande principer som ska följas vid behandling av personuppgifter. Den som är personuppgiftsansvarig ska bland annat följa principen om integritet och konfidentialitet. Denna säkerhetsprincip innebär att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.[446]

Det skydd som ska uppnås genom användning av lämpliga tekniska eller organisatoriska[447] säkerhetsåtgärder i förhållande till behandlingens art, omfattning, sammanhang och ändamål samt de risker som behandlingen medför.[448]

Detta innebär, åtminstone i teorin, att en personuppgiftsansvarig, när det är lämpligt, ska säkerställa förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft av de system och tjänster som används för att behandla personuppgifter. Vidare åläggs den som behandlar uppgifterna att säkerställa förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident. Det ska också finnas ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.[449]

Uppgifter om personers hälsa, sexualliv eller sexuella läggning är exempel på känsliga personuppgifter. Som huvudregel förbjuder dataskyddsförordningen behandling av sådana särskilda kategorier av personuppgifter, så kallade känsliga personuppgifter, men det finns undantag. Hälso- och sjukvården och omsorgen utgör ett sådant undantag.[450] Den rättsliga grunden för detta återfinns bland annat i 3 kap. 5 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.[451]

---

444 11 och 17 §§ förordningen om behandling av personuppgifter inom socialtjänsten.

445 Definitionen i artikel 4.8 i dataskyddsförordningen och exempelvis skyldigheten att vidta lämpliga säkerhetsåtgärder i artikel 32.

446 Artikel 5.1 f i dataskyddsförordningen.

447 Till tekniska åtgärder räknas till exempel brandväggar, kryptering, pseudonymisering, säkerhetskopiering och antivirusskydd. Organisatoriska åtgärder handlar till exempel om interna rutiner, instruktioner och riktlinjer.

448 Se artikel 5.1 f och artikel 32.1 dataskyddsförordningen.

449 Artikel 32,1 b, c och d dataskyddsförordningen. Eventuella biträden som ansvarig väljer att använda sig av har samma skyldigheter.

450 Artikel 9.1 h och 9.3 dataskyddsförordningen. Se även dåvarande Datainspektionen 2020, *Behovs- och riskanalys inom hälso- och sjukvården – en vägledning*, s. 4.

451 Förutsatt att behandlingen är nödvändig för förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård eller behandling, social omsorg, eller förvaltning av hälso- och sjukvårdstjänster, social omsorg samt deras system. Detta framgår även i 2 kap. 7 a § patientdatalagen under förutsättning att krav på tystnadsplikt kan upprätthållas.

Enligt dataskyddsförordningen ska den personuppgiftsansvarige anmäla personuppgiftsincidenter till den ansvariga tillsynsmyndigheten[452], som är Integritetsskyddsmyndigheten (IMY).[453] En personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[454]

Nationella bestämmelser avseende vård och omsorg som kompletterar dataskyddsförordningen

Patientdatalagen (2008:355) (PDL) kompletterar dataskyddsförordningen och innehåller sektorsspecifika bestämmelser vid behandling av personuppgifter inom hälso- och sjukvården som bedrivs av regioner och kommuner samt annan juridisk person eller enskild näringsidkare. PDL kompletteras av bland annat patientdataförordningen (2008:360) och Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).[455] Bestämmelserna[456] preciserar kraven på sjukvårdshuvudmännen och på personuppgiftsansvariga inom vården vad gäller behandling och skydd av patientinformation.[457] Det rör sig inte bara om skydd för enskildas integritet utan också om skydd som ska säkerställa kvaliteten i verksamheten och allmänhetens förtroende för densamma, framför allt om informationsstödet i form av system och elektroniska rutiner är en integrerad del av verksamheten och en förutsättning för att upprätthålla uppsatta kvalitetsmål.[458]

Enligt PDL ska informationshanteringen inom hälso- och sjukvården vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet.[459] Bestämmelserna i PDL rör bland annat den så kallade inre sekretessen, som innebär att den som arbetar hos en vårdgivare får ta del av uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården.[460] Detta förtydligas genom att det ställs krav på vårdgivare gällande behörighetstilldelning och åtkomstkontroll, som gäller även vid sammanhållen journalföring.[461] Vårdgivarens

452 Artiklarna 33.1 och 51.1 dataskyddsförordningen.
453 2 a § förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten.
454 Artikel 4.12 dataskyddsförordningen.
455 Nationell lagstiftning kan endast komplettera och fylla ut dataskyddsförordningen. När personuppgifter behandlas måste vårdgivare tillämpa dataskyddsförordningens bestämmelser och därefter tillämpa den kompletterande lagstiftningen om den är förenlig med dataskyddsförordningen.
456 Nationella bestämmelser som kompletterar dataskyddsförordningens krav på säkerhet återfinns främst i 4 och 6 kap. patientdatalagen samt 3 och 4 kap. Socialstyrelsens föreskrifter, HSLF-FS 2016:40.
457 25 kap. 1 § offentlighets- och sekretesslagen.
458 Se Manólis Nymark, Patientdatalagen – En kommentar [3.1 Juno version 2]. Nymark hävdar att brister i it-säkerhetsmiljön i förlängningen leder till vårdskador enligt patientsäkerhetslagen.
459 1 kap. 2 § patientdatalagen.
460 4 kap. 1 § patientdatalagen.
461 4 kap. 2, 3 §§ och 5 kap. 7 § patientdatalagen. Se även 4 kap. 2 § Socialstyrelsens föreskrifter (HSLF-FS 2016:40).

beslut om tilldelning av behörighet ska föregås av en behovs- och riskanalys.[462] Vid tilldelning av behörighet framgår det av förarbetena till PDL att det ska finnas olika behörighetskategorier i journalsystemet.[463]

I Socialstyrelsens föreskrifter framgår bland annat att vårdgivaren genom ledningssystemet ska säkerställa att personuppgifterna är tillgängliga, riktiga, konfidentiella och spårbara.[464] Vårdgivare rekommenderas att använda ledningssystem för informationssäkerhet som bygger på ISO/IEC 27000-serien.[465] Vidare ska vårdgivaren kontrollera att informationssystem som används för behandling av personuppgifter inte riskerar personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet.[466]

För behandling av personuppgifter inom omsorgen finns bestämmelser som kompletterar dataskyddsförordningen. Dessa finns i lagen (2001:454) om behandling av personuppgifter inom socialtjänsten, i socialtjänstlagen (2001:453) och i förordningen (2001:637) om behandling av personuppgifter inom socialtjänsten. Rättsliga bestämmelserna anger främst vilka verksamheter som får behandla personuppgifter och hur personuppgifter får användas inom socialtjänsten. Den 1 mars 2024 kompletterades lagen om behandling av personuppgifter i socialtjänsten med bestämmelser som reglerar behörighetstilldelning och kontroll av sådana behörigheter.[467]

Lagen (2022:913) om sammanhållen vård- och omsorgsdokumentation innehåller bestämmelser som anger under vilka förutsättningar hälso- och sjukvården och socialtjänsten får använda ett elektroniskt system som gör det möjligt för en vårdgivare eller omsorgsgivare att ge eller få tillgång, genom direktåtkomst eller annat elektroniskt utlämnande, till personuppgifter hos andra vårdgivare eller omsorgsgivare.[468] För omsorgens del riktar bestämmelserna in sig på de delar av verksamheter som avser omsorg om äldre personer och personer med funktionsnedsättning.[469] Även den nämnda lagen ställer krav på begränsning av behörigheter och kontroll av åtkomst, och ger en patient eller en omsorgsmottagare rätt att motsätta sig viss behandling av personuppgifter.

462 4 kap. 1–3 och 9 §§ Socialstyrelsens föreskrifter (HSLF-FS 2016:40).

463 Prop. 2007/08:126 s. 148–149.

464 3 kap. 2 § Socialstyrelsens föreskrifter (HSLF-FS 2016:40).

465 3 kap. 2 § Socialstyrelsens föreskrifter och allmänna råd) om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

466 3 kap. 10 § Socialstyrelsens föreskrifter och allmänna råd) om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

467 Den 1 mars 2024 infördes nya bestämmelse som innebär krav på behörighetstilldelning och kontroll av åtkomst, se 10 § lagen om behandling av personuppgifter inom socialtjänsten, prop. 2022/23:131, bet. 2023/24:SoU3, rskr. 2023/24:46.

468 Definition av sammanhållen vård- och omsorgsdokumentation i 1 kap. 1 § i den nämnda lagen.

469 Prop. 2021/22:177, bet. 2021/22:SoU30, rskr. 2021/22:381.

Informationssäkerhet i nätverk och informationssystem för vården regleras i NIS-lagen

Bestämmelser som syftar till att säkerställa en hög grad av säkerhet i hälso- och sjukvårdens nätverk och informationssystem[470] regleras i lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (den så kallade NIS-lagen) och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-förordningen).[471] Genom lagen och förordningen har bland annat MSB och Socialstyrelsen bemyndigats att utfärda föreskrifter på området. IVO ska utöva tillsyn av de delar av NIS-lagen som berör hälso- och sjukvården och utifrån Socialstyrelsens föreskrifter på området. Leverantörer av samhällsviktiga tjänster inom hälso- och sjukvårdssektorn omfattas av NIS-lagen om antalet legitimerad vårdpersonal överstiger 50 årsarbetskrafter eller om minst 20 000 expedieringar av receptbelagda läkemedel utförs per år.[472]

Enligt NIS-lagen ska leverantören, det vill säga vårdgivare inom hälso- och sjukvården, vidta ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverk och informationssystem[473] som använder, lagrar och delar personuppgifter. Åtgärderna ska säkerställa att nivån på säkerheten i nätverk och informationssystem är lämplig i förhållande till risken.[474]

För att uppnå den säkerhet som NIS-lagen föreskriver ska leverantören bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete som omfattar bland annat en riskanalys och en åtgärdsplan som uppdateras årligen.[475] Vidare ska leverantören säkerställa kontinuiteten genom att arbeta förebyggande i syfte att minimera verkningar av incidenter som påverkar nätverk och informationssystem.[476] Enligt MSB:s föreskrift ska varje leverantör bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av standarderna SS-EN ISO/IEC 27001:2017 och SS-EN ISO/IEC 27002:2017 om ledningssystem för informationssäkerhet eller motsvarande.[477] Som tidigare nämnts rekommenderar även Socialstyrelsen

---

470 Kraven i NIS-lagen gäller inte organisationen i sin helhet utan enbart hanteringen av de nätverk och informationssystem som hanterar den samhällsviktiga tjänsten.

471 NIS har sin grund i Europaparlamentets och rådets direktiv (EU) 2016/1148 fastställer åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen, i syfte att förbättra den inre marknadens funktion (NIS-direktivet).

472 7 kap. (MSBFS 2021:9), Myndigheten för samhällsskydd och beredskaps föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster.

473 Med säkerhet avses nätverks och informationssystems förmåga att vid en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverk och informationssystem. Se 2 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

474 1och 13 §§ lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

475 11–12 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

476 14 § lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

477 5 § Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (MSBFS 2018:8).

ledningssystem utifrån standarden ISO/IEC 27000-serien och föreskriver också regler för drift, upphandling, utveckling och fysiskt skydd av informationssystem.[478]

Vårdgivare inom hälso- och sjukvården ska enligt NIS-lagen rapportera incidenter[479] som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten som de tillhandahåller.[480] Rapporteringen ska göras till MSB som skickar rapporteringen vidare till Socialstyrelsen och den ansvariga tillsynsmyndigheten IVO.[481]

EU fattade i december 2022 beslut om ett nytt NIS-direktiv, NIS 2, som ska ersätta de nuvarande nätverks- och informationssäkerhetsreglerna. Det nya direktivet innebär flera förändringar. Bland annat kommer fler sektorer, verksamheter och underleverantörer omfattas och rapporteringsskyldigheten effektiviseras för att undvika överrapportering. Vidare skärps kraven på aktörer genom minimikrav för åtgärder som ska tillämpas för att hantera risker som är kopplade till säkerheten i respektive aktörs nätverk och informationssystem.[482] Vad NIS 2-direktivet kommer att innebära för den svenska hälso- och sjukvården och socialtjänsten är fortfarande inte klart. En utredning om genomförandet av NIS2-direktivet i svensk rätt tillsattes den 2 mars 2023.[483] Enligt utredningsdirektivet ska utredaren bland annat ta ställning till om kommunerna eller delar av kommunernas verksamheter ska omfattas av regleringen. NIS 2-direktivet trädde i kraft den 16 januari 2023 vilket innebär att medlemsstaterna har 21 månader på sig att införliva NIS 2 i nationell lagstiftning, det vill säga 17 oktober 2024

MSB:s föreskrifter som berör informationssäkerhet rekommenderas till regioner och kommuner

Med stöd av förordningen (2022:524) om statliga myndigheters beredskap[484] har MSB utfärdat föreskrifter om att statliga myndigheters informationssäkerhet och informationshanteringssystem ska uppfylla grundläggande och särskilda säkerhetskrav.[485] Motsvarande föreskrifter finns inte för regioner och kommuner

478 4 kap. 3, 7, 9, 11 och 14 §§ Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

479 Med incident avses en händelse med en faktisk negativ inverkan på säkerheten i nätverk och informationssystem. Se 2 § punkt 10 lagen om informationssäkerhet för samhällsviktiga och digitala tjänster.

480 3, 18 §§ lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, 4 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

481 12 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

482 Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

483 Dir. 2023:30.

484 13 och 26 §§ förordningen (2022:524) om statliga myndigheters beredskap.

485 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS:2020:6).

men MSB rekommenderar regioner och kommuner att använda sig av föreskrifterna i sitt informationssäkerhetsarbete.[486]

MSB:s föreskrift om informationssäkerhet för statliga myndigheter ställer krav på ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av internationella standarder.[487] Där föreskrivs att arbete med informationssäkerhet ska involvera ledningen, grundas på risk- och sårbarhetsanalyser och omfatta åtgärder så som informationsklassning utifrån begreppen konfidentialitet, riktighet och tillgänglighet. Vidare ska man också ansvara för personalens informationsbehandling och åtgärder för att upprätthålla kontinuitet under incidenter och kriser.[488]

I MSB:s föreskrift om säkerhetsåtgärder i informationssystem för statliga myndigheter ställs krav på vad varje myndighet minst behöver göra för att uppnå en godtagbar nivå av säkerhet i sina IT-system. MSB ställer uttryckliga krav på en rad utpekade IT-säkerhetsåtgärder som bedöms vara en del av ett grundskydd för IT-miljön. Det ställs bland annat krav på att det ska finnas en ansvarig person för varje informationssystem. Myndigheten måste arbeta riskbaserat i sin förvaltning av informationssystemen, förhindra spridning av incidenter och arbeta med att minska konsekvenserna av angrepp, bland annat genom att arbeta aktivt med behörigheter, kryptering, säkerhetskonfigurering och säkerhetskopiering.[489]

---

486 Se till exempel MSB, ”Nya föreskrifter och stöd på informationssäkerhetsområdet”, hämtad 2022-12-16 och MSB, ”Informationssäkerhet i fokus – Webbinarie 1: En praktisk introduktion”, hämtad 2022-12-16.

487 SS-EN ISO/IEC 27001:2017 Informationsteknik - Säkerhetstekniker - Ledningssystem för informationssäkerhet, och SS-EN ISO/IEC 27002:2017 Informationsteknik - Säkerhetstekniker - Riktlinjer för informationssäkerhetsåtgärder.

488 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS:2020:6).

489 Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Bilaga 2. Urval och metod

I bilagan redogör vi för urval av regioner och kommuner samt för genomgången av inkomna frågor från vård- och omsorgsgivare och myndigheternas svar.

Sex kommuner och två regioner i två län som hanterar stora mängder personuppgifter i landet

Vi har undersökt hur de statliga insatserna för att stödja regionernas och kommunernas informationssäkerhetsarbete har fungerat i två län. Vi har intervjuat företrädare för regionen och tre kommuner i de två länen. Syftet har varit att förstå hur de arbetar med informationssäkerhet för personuppgifter inom vården och omsorgen, hur det statliga stödet och vägledningen bidrar till deras arbete och vilka behov av stöd som de har för att höja nivån på sin informationssäkerhet. Därutöver har vi också intervjuat företrädare för en kommun som utsatts för ett cyberangrepp i december 2022. Syftet har varit att granska vilket stöd som de fått från myndigheter vad gäller hantering av den uppkomna IT-incidenten och dess konsekvenser.

Urvalet av regioner och kommuner har i huvudsak gjorts utifrån befolkningsstorlek och det omfattar regionen och tre kommuner i två län. Vi har valt ut de två största länen som tillsammans omfattar 40 procent av befolkningen. Befolkningsmässigt är de två länen olika stora med en blandning av stora och små kommuner. Vi har utgått från att regioner med störst befolkningsstorlek hanterar stora mängder personuppgifter om enskilda och från att konsekvenserna av bristande skydd därmed omfattar många individer. Vi har också tagit hänsyn till kommunstorleken i regionen så att urvalet omfattar små-, medelstora och stora kommuner. Syftet har varit att få en bild av olika kommuners förutsättningar för att arbeta systematiskt med informationssäkerhet, såsom resurser och kompetens.

Tabell 3 Regioner och kommuner som ingår i intervjuundersökningen

Namn[490]	Datum för intervju	Storlek (befolkning)	Region
Kommun 1	2023-06-07	Stor	Region 1
Kommun 2	2023-06-15	Liten	Region 2
Kommun 3	2023-06-16	Stor	Region 2
Kommun 4	2023-06-16	Medel	Region 2
Kommun 5	2023-06-19	Liten	Region 1
Kommun 6	2023-06-27	Medel	Region 1
Kommun 7	2023-06-28	Liten	(cyberangrepp)[491]
Region 1	2023-06-09	Stor	-
Region 2	2023-06-21	Stor	-

490 Regionerna och kommunerna har anonymiserats i noterna i granskningsrapporten.

491 Kommunen drabbades av ett cyberangrepp i december 2022 vilket fått konsekvenser för bland annat skyddet av personuppgifter.

Vi har genomfört sammanlagt 9 semistrukturerade intervjuer med företrädare för de utvalda kommunerna och regionerna. Vid respektive region och kommun har vi intervjuat anställda på centralnivå, exempelvis statledningskontor, som arbetar med informationssäkerhet och innehar titel såsom informationssäkerhetsansvarig, informationssäkerhetssamordnare, informationssäkerhetschef eller digitaliseringsstrateg. Regionerna och de större kommunerna har ofta förvaltningar eller nämnder som bedriver bland annat vård- och omsorgsverksamheter och de har eget ansvar för informationssäkerhet. I sådana fall finns styrande dokument och riktlinjer för informationssäkerhetsarbetet från centralnivån som de måste förhålla sig till, men det är de själva som ansvarar för informationssäkerhetsarbetet.

Analys av inkomna frågor från vården och omsorgen

Vård- och omsorgsgivare kan ställa frågor om regelverket och informationssäkerhet till IMY, Socialstyrelsen och MSB för att få stöd. För att bedöma vilket stöd de fått har vi gått igenom dessa frågor och myndigheternas svar.

Mellan 2018 och 2022 svarade IMY på cirka 200 kvalificerade frågor från vårdgivare och omsorgsgivare i kommuner samt cirka 80 kvalificerade frågor från vårdgivare i regioner.[492] Av cirka 280 kvalificerade frågor har Riksrevisionen tagit del av 53 frågor, varav de flesta från 2022. Urvalet har gjorts av medarbetare på IMY eftersom det inte har gått att söka på frågor från vård- och omsorgsgivare i IMY:s diariesystem. De sammanställda uppgifterna baseras på ett strategiskt urval och bör tolkas med viss försiktighet. Riksrevisionens urval inkluderar frågor från avsändare i kommuner och regioner så som IT-avdelningar, kommunförbund, socialnämnder och omsorgsförvaltningar.

Under hösten 2022 till och med december 2022 fick MSB in och besvarade totalt 40 frågor, varav 26 frågor från kommuner och 2 från regioner. Vi har gått igenom samtliga frågor. Majoriteten av frågorna handlade om det systematiska informationssäkerhetsarbetet och hur man ska införa säkerhetsåtgärder i den egna specifika verksamheten.[493]

Socialstyrelsen har inte lämnat underlag till Riksrevisionen om inkomna frågor från vården och omsorgen eller myndighetens svar. Det beror på att Socialstyrelsens ärendehanteringssystem inte är anpassat för att kunna göra uppföljningar av vilka som har mejlat eller ringt eller vilka frågor som de har ställt och vilka svar som har lämnats. Det är inte heller möjligt att ta fram statistik över hur många frågor som inkommer från regioner och kommuner eller vad frågorna handlar om.[494]

---

492 Under samma period svarade IMY också på cirka 750 frågor av enklare slag från kommunerna och cirka 150 frågor från regionerna.

493 Att bygga systematiskt informationssäkerhetsarbete (10); Säkerhetsåtgärder (5); CISO-rollen (3); Riskhantering; Klassning av information; Ledning och styrning (2 vardera); Utbildningar; Uppföljning och förbättring; Utforma incidentrapportering (1 vardera).

494 Intervju med företrädare för Socialstyrelsen, 2023-04-13.

EN GRANSKNINGSRAPPORT FRÅN RIKSREVISIONEN

Informationssäkerhet i vård och omsorg – statens stöd och tillsyn (RiR 2024:6)

Vård- och omsorgsgivare hanterar stora mängder känsliga personuppgifter digitalt och ansvarar för att skydda dem. Riksrevisionen har granskat statens arbete för att stödja och kontrollera vård- och omsorgsgivares informationssäkerhet. Riksrevisionens övergripande slutsats är att de statliga insatserna inte är effektiva.

Myndigheten för samhällsskydd och beredskaps (MSB:s), Integrationsmyndighetens (IMY:s) och Socialstyrelsens stöd är inte tillräckligt anpassat efter vård- och omsorgsgivares behov, särskilt när det gäller säkerhetsåtgärder som krävs för att uppnå tillräckligt skydd. Det beror bland annat på att ingen av myndigheterna anser sig ha ansvar för att ta fram ett sektorsanpassat stöd, samt att regeringen inte har tydligt fastställt ansvars- och uppgiftsfördelningen mellan myndigheterna. Myndigheterna gör sällan rättsliga ställningstaganden för hur bestämmelserna som gäller för vård- och omsorgsgivare kan tolkas och vad de innebär i praktiken. En annan brist är att IMY:s och Inspektionen för vård och omsorgs (IVO:s) tillsyn har varit begränsad och exempelvis inte omfattat omsorgsgivare, vilket gjort att den inte på ett effektivt sätt kontrollerat informationssäkerheten för personuppgifter. Dessutom är tillsynen bara delvis riskbaserad, vilket gör att det är svårt att bedöma om den fokuserar på verksamheter där den skulle ge störst nytta.

Riksrevisionen rekommenderar regeringen att bland annat förtydliga Socialstyrelsens ansvar för att ta fram verksamhetsanpassat stöd till vårdens och omsorgens informationssäkerhetsarbete. IMY rekommenderas bland annat att effektivisera handläggningen och bedriva mer riskbaserad tillsyn. IVO rekommenderas bland annat att bedriva tillsyn som granskar om vårdgivare uppfyller NIS-lagens samtliga krav på säkerhet i nätverk och informationssystem.

RIKS REVISIONEN

Riksrevisionen
www.riksrevisionen.se
S:t Eriksgatan 117
Box 6181, 102 33 Stockholm
08-5171 40 00