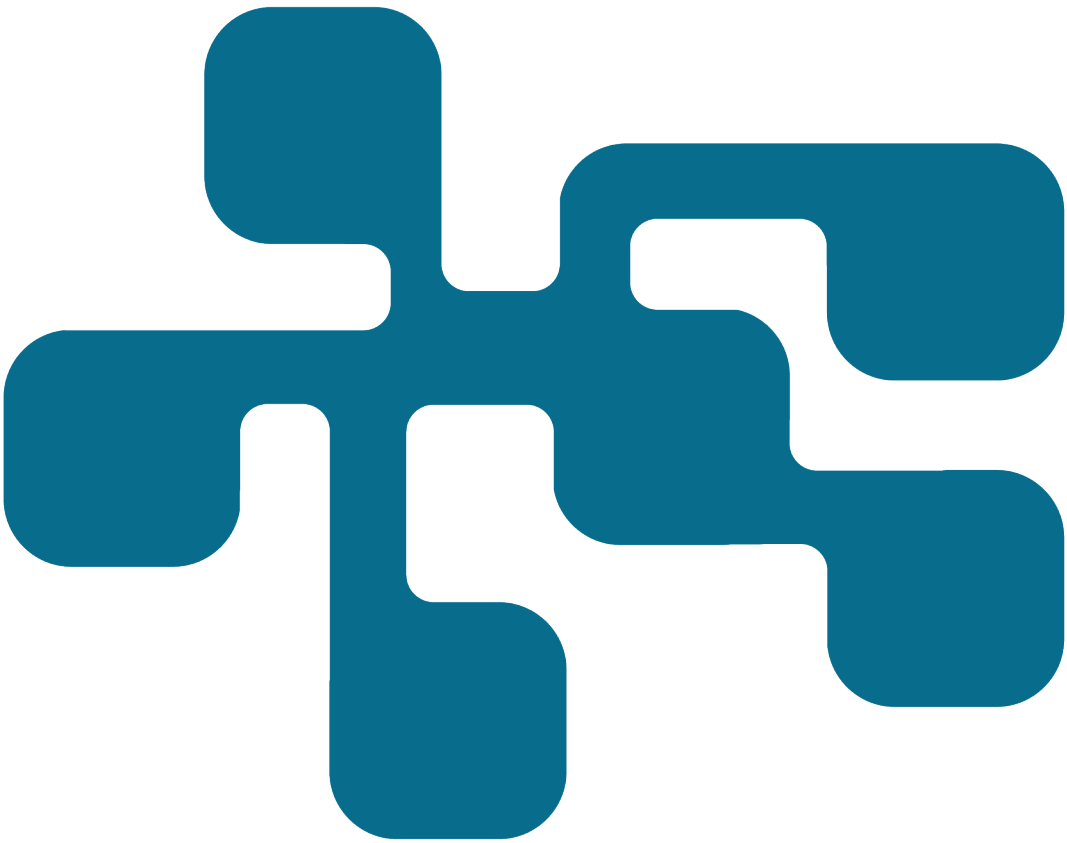
NCS3 - Patient- och cybersäkerhet rörande medicintekniska produkter

En NCS3-studie om avvikelsehantering och CE-märkning

Ulrika Eckersand, Eva Mittermaier,
Ann-Sofie Stenérus Dover och Johanna Wahrenberg

FOI
MSB



FOI-R--5226--SE
MSB 2021-02578
ISSN 1650-1942

December 2021

Ulrika Eckersand, Eva Mittermaier, Ann-Sofie Stenérus Dover och Johanna Wahrenberg

Patient- och cybersäkerhet rörande medicintekniska produkter

En NCS3-studie om avvikelsehantering och CE-märkning

Titel	Patient- och cybersäkerhet rörande medicintekniska produkter – En NCS3-studie om avvikelsehantering och CE-märkning
Title	Safety and cybersecurity in medical devices
Rapportnr/Report no	FOI-R--5226--SE
Månad/Month	December
Utgivningsår/Year	2021
Antal sidor/Pages	64
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E13769
Godkänd av/Approved by	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Sjukvården digitaliseras precis som det övriga samhället. För medicintekniska system och produkter kan digitaliseringen få konsekvenser för såväl patientsäkerheten som cybersäkerheten. EU har beslutat om två förordningar (MDR och IVDR) med syfte att förbättra patientsäkerhet i medicintekniska produkter. Förordningarna påverkar arbetet med bland annat certifiering och avvikelsehantering.

Intervjuer med regioner, myndigheter, tillverkare och anmälda organ har genomförts under 2021. Resultaten av dessa intervjuer bekräftar att regelverket påverkar cybersäkerheten. Ibland är regelverket grund för att både patientsäkerhet och cybersäkerhet förbättras och ibland motverkar regelverket cybersäkerheten. Enligt MDR klassificeras vårdens informationssystem som medicintekniska produkter. Medicinteknisk personal behöver därmed samarbeta närmre informations-, säkerhets- och IT-säkerhetsavdelningar.

Det finns ett stort behov av personal med rätt kompetens hos tillverkare, vårdgivare och anmälda organ. Den kompetens som krävs är komplex och omfattar patientsäkerhet, cybersäkerhet samt regelverk och certifieringsarbete. Det är stor brist på anmälda organ, och utan personalresurser och rätt kompetens riskerar de anmälda organen att inte räcka till för de produkter som ska ut på marknaden.

Avvikelserapporteringen behöver öka, särskilt till den nationella databasen reidarMTP, som ska vara en källa till kunskap om avvikelser i hela landet. Att rapportera till reidarMTP kräver tid, men andra uppgifter prioriteras högre. För att förbättra rapporteringen av cyberrelaterade avvikelser behövs mer samarbete mellan medicinteknisk och IT-personal.

Nyckelord: avvikelse, certifiering, cybersäkerhet, Medicinteknisk produkt, NCS3, patientsäkerhet

Summary

Digitalization of the health care sector is being implemented at high speed, and has consequences for both safety and cyber security. The European Union have decided on two new regulations (MDR and IVDR) with the purpose of improving safety of medical devices. These two new EU regulations influence the work with certifications and with reporting medical device problems.

In this study, representatives of care providers (operated by regional councils), authorities, manufacturers, and notified bodies were interviewed. The results of the interviews confirms the presumption that the legal framework has impact on cyber security. Sometimes both safety and cyber security are improved, and sometimes the legal framework counteracts cyber security. MDR classifies healthcare information systems as medical device. Biomedical engineers therefore must work closer to information security departments.

There is a need for personnel with proper competence from manufacturers, care providers and notified bodies. The competence needed comprises safety, cyber security, legal framework and certification work. There is a lack of notified bodies in Sweden, and without personnel and proper competence there is a risk that the notified bodies are not being able to certify enough products for the market.

The reporting of medical device problems must improve, especially to the national database reidarMTP. Reporting to reidarMTP is time consuming and other assignments are prioritized.

Keywords: certification, deviation, cyber security, EUDAMED, IVDR, MDR, Medical device, safety

Innehåll

1 Inledning

Som en viktig del i att hantera frågor kring säkerhet i cyberfysiska system har Myndigheten för samhällsskydd och beredskap, MSB, och Totalförsvarets forskningsinstitut, FOI, i samarbete byggt upp Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3). Cybersäkerhet i medicintekniska produkter faller inom ramen för detta arbete.

Medicintekniska produkter och medicintekniska informationssystem är system som används dagligen i hälso- och sjukvården, och som ibland är livsavgörande. De omgärdas därför av omfattande regelverk. Till dessa regelverk hör certifieringssystem[1]. CE-märkning[2] av medicintekniska produkter har stor betydelse för en god patientsäkerhet, men innebär även vissa utmaningar för cybersäkerheten.

Patientsäkerhet innebär enligt 1 kap. 5-6 § patientsäkerhetslagen (2010:659) skydd mot vårdskada i patienters kontakt med hälso- och sjukvården.

För att öka patientsäkerheten i hälso- och sjukvården rapporteras avvikelser, det vill säga tillbud eller negativa händelser, som rör medicintekniska produkter. Dessa ska göras till Läkemedelsverket. För bästa kunskapsspridning bör avvikelser också rapporteras till den rikstäckande databasen reidarMTP. Den nya EU-förordningen Medical Device Regulation 2017/745 (MDR) innebär utökade krav på tillverkare att också rapportera olyckor och tillbud till den europeiska databasen European Database on Medical Devices (EUDAMED).

Under 2020 genomförde FOI en studie i två delar om cybersäkerhet i medicintekniska produkter och medicintekniska informationssystem. I den första delstudien var fokus på att analysera inrapporterade avvikelser i reidarMTP där ett av resultaten visade en trend av minskad avvikelserapportering till databasen. Endast ett fåtal av de avvikelser som rapporterades kunde klassas som cyberrelaterade. Den andra delstudien fokuserade på faktainsamling avseende regelverk, standarder och certifiering av MTP. Faktainsamlingen visade att det finns ett omfattande regelverk med bland annat två nya EU-förordningar: den ovan nämnda MDR, som började gälla i maj 2021, och In Vitro Diagnostic Regulation 2017/746 (IVDR), som börjar gälla i maj 2022. Att förhålla sig till ett stort antal standarder kräver både tid och kunskap hos tillverkare och vårdgivare.[3]

Studien 2020 har lagt grunden till den intervjustudie som presenteras i denna rapport om hur vårdgivare, företag och myndigheter arbetar med cybersäkerhet rörande medicintekniska produkter. Dels handlar det om avvikelsehantering, särskilt cyberrelaterade avvikelser, dels beskriver rapporten hur medicinteknisk

[1] Certifiering innebär att en organisation, produkt eller person bedöms uppfylla krav som ställs i standarder eller andra styrdokument (Myrén, 2020).
[2] Produktsäkerhetscertifiering som har lagstadgats av EU Se kap 2.3.
[3] För mer information om studierna från 2020 hänvisas till bilagorna 1 och 3 samt de båda memon som skrevs: Eckersand & Wahrenberg (2021) och Eckersand & Wahrenberg (2020).

personal, i samverkan med IT-personal, arbetar med cybersäkerhet. Detta omfattar även hur personalen arbetar med att öka inrapporteringsgraden till den nationella avvikelsedatabasen. I denna studie presenteras också hur regelverk och certifieringsmöjligheter förhåller sig till patientsäkerhet och cybersäkerhet.

1.1 Studiens mål och syfte

Målet för denna studie är tredelat. Det första målet är att studera hur regelverk och certifiering (särskilt CE-märkning) förhåller sig till patientsäkerhet och cybersäkerhet. Det andra målet är att analysera hur de nya EU-förordningarna kan komma att påverka arbetet med medicintekniska produkter och medicintekniska informationssystem. Det tredje målet är att följa upp 2020 års studie om avvikelser för att analysera hur medicinteknisk personal arbetar med avvikelsehantering (framför allt rapporteringen till den nationella databasen reidarMTP) med särskilt fokus på cyberrelaterade avvikelser.

Dessa mål syftar till att ge underlag till informationsmaterial som i första hand vänder sig till vårdgivare och i andra hand kan användas i vårdgivarnas upphandlingsprocess. Målgrupper för rapporten är i huvudsak medicinteknisk personal och IT-personal. Ett annat syfte med studien är att ta fram underlag till att sprida framgångsfaktorer för arbetet med medicintekniska produkter och de regelverk som gäller för dessa.

1.2 Metod

Denna studie är i huvudsak en intervjustudie och omfattar intervjuer med fem svenska regioner, tre företag som tillverkar medicintekniska produkter och som är verksamma i Sverige, Inspektionen för vård och omsorg (IVO), Läkemedelsverket samt det statliga forskningsinstitutet RISE.

De intervjuade regionerna är Jämtland Härjedalen, Gävleborg, Sörmland, Uppsala och Västra Götaland. Urvalet är gjort i samråd med MSB för att få en variation i storlek och hur långt olika vårdgivare i regionerna har kommit i arbetet med cybersäkerhet. De intervjuade personerna i regionerna representerar olika roller såsom enhetschef, riskhanteringssamordnare, säkerhetssamordnare, förvaltningsledare och specialist inom medicinteknik, enhetschef inom IT-drift samt informations- och IT-säkerhetsansvarig person. Alla tillfrågade regioner har velat delta med motivering att cybersäkerhet i medicintekniska produkter är ett oerhört viktigt område som de vill vara delaktiga i att utveckla.

I Sverige finns det såväl stora globala medicintekniska industriföretag som små företag. De intervjuade företagen har valts ut i samverkan med MSB och på förslag från branschorganisatinen Swedish Medtech. Företagen har också rekommenderat oss att prata med andra företag som har andra typer av produkter. Alla tillfrågade företag har inte velat delta. De intervjuade personerna på företagen representerar

olika roller som kvalitetsansvarig, cybersäkerhetsansvarig, dataskyddsombud tilllika informationssäkerhetschef, säkerhetsarkitekt och marknadschef.

För att förstå hur certifieringarna kommer att fungera med det nya regelverket, hade det också varit önskvärt att intervjua något av de anmälda organ[4] som certifierar enligt de nya medicintekniska regelverken. Inget av de anmälda organen som verkar som sådant gentemot företag i Sverige och som certifierar enligt det nya regelverket har dock ställt upp på intervju. En intervju med RISE, som föreslås bli ett anmält organ enligt den nya förordningen, har genomförts och får representera anmälda organ i denna studie. RISE certifierar dock enligt det gamla regelverket (EU-direktivet Medical Device Directive, MDD) och intervjusvaren ska därför ses med MDD som utgångspunkt.

På myndigheterna och på RISE har chefer och samordningsansvariga för frågor som rör medicintekniska produkter intervjuats. Läkemedelsverket utövar tillsyn över medicintekniska produkter och organ som ger CE-märkning samt är ansvarig myndighet för medicintekniska produkter och avvikelserapportering.[5] Inspektionen för vård och omsorg, IVO, har tillsyn av vård och omsorg och så kallade egentillverkade medicintekniska produkter. IVO:s ansvar omfattar patientsäkerhet, informationssäkerhet samt avvikelsehantering.[6]

Med anledning av covid-19 har intervjuerna genomförts via telefon och videolänk.

Intervjufrågorna som har använts är i huvudsak hämtade från de två memon som ingick i studien 2020. (Se *Bilaga 1. Intervjufrågor*.)

Intervjuerna refereras i texten på olika sätt. För de båda myndigheterna och RISE anges vilken aktör som säger vad. För de intervjuer som har genomförts med regioner hänvisas till att det är en eller flera regioner som uttalar sig (ibland refereras till om det är medicinteknisk eller IT-teknisk personal som uttalar sig). Även för företagen hänvisas endast till att det är ett företag som uttalar sig. Enskilda personer anges inte av integritetsskäl. Undantag görs för de intervjuer som gjordes under 2020 i förstudien till denna studie. Där intervjuades personerna specifikt för den roll de har.

I rapporten återges även åsikter från branschföreningar som har uttalat sig bland annat i media kring dessa frågor.

[4] *Anmälda organ, Notified Bodies,* är oberoende företag och organisationer som bistår och övervakar tillverkarnas arbete med att verifiera att produkterna uppfyller EU:s regelverk.
[5] Instruktion för Läkemedelsverket, SFS 2020:57.
[6] Instruktion för Inspektionen för vård och omsorg, SFS 2013:176.

1.3 Avgränsningar

Denna studie fokuserar på medicintekniska produkter inom ramen för MDR. Hos medicintekniska produkter för in vitro-diagnostik finns särskilda egenskaper gällande exempelvis riskklassificering och klinisk evidens som kräver en särskild lagstiftning, vilken skiljer sig från lagstiftningen för andra medicintekniska produkter (IVDR, 2017). In vitro-diagnostik-produkter och IVDR omnämns i rapporten endast för förståelsen av helheten och utmaningarna med de nya regelverken. Ingen djupare analys av specifikt IVDR görs.

Studien omfattar sådan hälso- och sjukvård som avses i 2 kap. 1 § 1 punkten i hälso- och sjukvårdslagen (2017:30):

> 1 § Med hälso- och sjukvård avses i denna lag
> 1. åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador,
> 2. sjuktransporter, och
> 3. omhändertagande av avlidna.
>
> Lagen omfattar inte tandvård enligt tandvårdslagen (1985:125).

Uppdraget omfattar således inte sjuktransporter och tandvård. Inte heller hjälpmedel och omsorg omfattas trots att produkter inom dessa områden är viktiga ur ett patient- och cybersäkerhetsperspektiv samt berörs av det nya regelverket.

Att besvara frågor om hur man specifikt arbetar med cybersäkerhet kan vara både företagshemligt och säkerhetskänsligt. Att sammanställa flera olika aktörers arbete med dessa frågor kan bli ännu känsligare. Önskemålet från uppdragsgivaren har varit en öppen rapport där resultatet kan presenteras och tillgängliggöras för en bred krets av läsare. Därför har cybersäkerhetsfrågorna i intervjuerna hållits på en övergripande nivå.

1.4 Disposition/Läsanvisning

Målgrupp för denna rapport är främst ansvariga för medicintekniska system inom hälso- och sjukvården, men den bör vara av intresse även för andra aktörer i vården samt för ansvariga för utveckling och användning av cyberfysiska system i stort. Några cybertekniska och medicintekniska termer och förkortningar får sin förklaring i *Bilaga 2. Begrepp och förkortningar*.

Kapitel *2 Regelverk* är en översiktlig sammanställning av det regelverk som direkt och specifikt hanterar medicintekniska produkter och certifiering av produkter. I detta kapitel redovisas också hur företagen, myndigheterna och RISE ser på regelverket.

Kapitel *3 Cybersäkerhet i vården* beskriver hur patient-, cyber- och informationssäkerhet hänger ihop i arbetet med medicintekniska produkter. Resultaten från intervjuerna med avseende på hur regionerna arbetar med dessa presenteras också.

I kapitel *4 Avvikelsehantering* presenteras de båda databaserna EUDAMED och reidarMTP. Därefter redogörs för de resultat från intervjuerna som rör avvikelserapportering och orsaker till minskad rapportering. Kapitlet avslutas med de intervjuade regionernas förslag på hur man kan förbättra avvikelserapporteringen.

I kapitel *5 Diskussion* diskuterar författarna några viktiga iakttagelser i resultaten, och avslutningsvis i kapitel *6 Slutsatser* dras några sammanfattande slutsatser från studien.

I *Bilaga 1. Förslag till intervjufrågor* finns de frågeförslag som togs fram under den tidigare studien 2020 och från vilka frågorna i intervjuerna i denna studie har hämtats.

I *Bilaga 2. Begrepp och förkortningar* får några cybertekniska och medicintekniska termer och förkortningar som används i denna rapport sin förklaring.

I *Bilaga 3. Standarder* görs en översiktlig sammanställning av standarder och en teknisk rapport som rör medicintekniska produkter och cybersäkerhet.

I *Bilaga 4. Avvikelsestatistik* redovisas delar av den statistik som publicerades i den förra studien 2020.[7]

[7] Eckersand & Wahrenberg (2021)

2 Regelverk

Medicintekniska produkter och medicintekniska informationssystem utgör en central del av hälso- och sjukvården, och deras funktion kan ibland vara livsavgörande. De omgärdas därför av omfattande regelverk, certifieringssystem och standarder. Flera föreskrifts- och tillsynsmyndigheter samt certifieringsorgan är inblandade för att säkerställa att medicintekniska produkter och informationssystem är säkra att använda. I det följande kapitlet ges en översiktlig beskrivning av regelverk, några av de standarder som gäller medicintekniska produkter samt allmänt om CE-märkning och specifikt CE-märkning av medicintekniska produkter. Utöver de nämnda regelverken och standarderna finns fler som direkt och indirekt påverkar medicintekniska produkter, till exempel elsäkerhetslagen i Sverige och andra regelverk i EU. Tillverkarna har också att förhålla sig till standarder på de övriga marknader där de verkar, bland andra de amerikanska kraven.

2.1 EU-förordningar och svenskt regelverk

De nya EU-förordningarna MDR och IVDR, som beslutades 2017 och som har trätt i kraft 2021 respektive träder i kraft 2022, blir till skillnad från EU-direktiv direkt svensk lag och ersätter därför de gamla EU-direktiven, den tidigare svenska lagen (1993:584) om medicintekniska produkter och de tillhörande föreskrifterna. EU-förordningarna kompletteras med en ny svensk lag, en ny förordning och nya föreskrifter inom det medicintekniska området (Mårtensson, 2019). Se Tabell 1.

Syftet med MDR och IVDR är att säkerställa att den inre marknaden för medicintekniska produkter har en hög hälsoskyddsnivå för patienter och användare. MDR syftar dessutom till att skapa ett starkt, transparent, hållbart och internationellt erkänt ramverk med förbättrad klinisk säkerhet och rättvist marknadstillträde för tillverkare (MDR, 2017) (IVDR, 2017). I de intervjuer vi har genomfört i denna studie finns det en samstämmig syn på att MDR kommer att bidra till att förbättra patientsäkerheten. I de båda förordningarna ställs vidare höga kvalitets- och säkerhetskrav på medicintekniska produkter för att öka de medicintekniska produkternas säkerhet (MDR, 2017) (IVDR, 2017).

Ett stort antal lagar, förordningar och föreskrifter styr olika typer av medicintekniska produkter. I det följande redovisas det regelverk som kompletterar MDR och som har trätt i kraft under de första sju månaderna 2021.

Tabell 1. Regelverk – EU-förordningar och svenskt regelverk rörande medicintekniska produkter.

Regelverk	Kortnamn	Typ av regel	Ikraftträdande
Medical Device Regulation, Regulation (EU) 2017/745	MDR[1]	EU-förordning	2021-05-26
In Vitro Device Regulation, Regulation (EU) 2017/746	IVDR[2]	EU-förordning	2022-05-26
Lag (SFS 2021:600) med kompletterande bestämmelser till EU:s förordning om medicintekniska produkter		Svensk lag	2021-07-15
Förordning (SFS 2021:631) med kompletterande bestämmelser till EU:s förordning om medicintekniska produkter		Svensk förordning	2021-07-15
Läkemedelsverkets föreskrifter om informations- och rapporteringsskyldighet avseende medicintekniska produkter, HSLF-FS 2021:32		Svensk föreskrift	2021-05-26
Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården, HSLF-FS 2021:52		Svensk föreskrift	2021-07-15

[1]MDR ersätter Rådets direktiv 93/42/EEG av den 14 juni 1993 om medicintekniska produkter.
[2]IVDR ersätter Europaparlamentets och Rådets direktiv 98/79/EG av den 27 oktober 1998 om medicintekniska produkter för in vitro-diagnostik.

2.2 Standarder

Dagens regelverk i EU bygger på utpekade så kallade harmoniserade standarder som produkterna ska följa. Lagstiftningens generella krav specificeras på så sätt i de harmoniserade standardernas tydligare och konkretare kravställningar (SIS, 2021). På detta sätt ska nationella särkrav inom EU undvikas, och lagstiftningen begränsas därmed till övergripande krav för bland annat säkerhet och hälsa, medan standarder ger en lägsta skyddsnivå när det gäller de krav som finns i lagstiftningen (SIS, 2021). Harmoniserade standarder används för att visa att vissa produkter eller

tjänster uppfyller de tekniska kraven i EU-lagstiftningen (EU, Standarder i Europa, 2020). Om en tillverkare av en medicinteknisk produkt uppfyller kraven i en harmoniserad standard, där kraven är avstämda mot regelverket, antas tillverkaren även uppfylla regelverkets motsvarande krav. Det betyder att en produkt som har tillverkats enligt en harmoniserad standard också kan godkännas av en svensk myndighet (Läkemedelsverket, 2013).

Det finns ett stort antal svenska standarder som beskriver medicintekniska produkter och som bygger på europeiska och internationella standarder. Det finns specifika standarder för olika medicintekniska produkter såsom dentala implantat och pacemakers, men även processtandarder som berör medicintekniska produkter generellt, såsom riskhantering, ledningssystem för kvalitet och märkning av medicintekniska produkter.

I *Bilaga 3. Standarder* görs en översiktlig sammanställning av standarder som kan vara relevanta för leverantörer och vårdgivare när det rör medicintekniska produkter och cybersäkerhet.

2.3 CE-märkning

En viktig del av marknadskontrollen är CE-märkning[8] och uppfyllande av olika standarder. I och med en CE-märkning intygar en tillverkare eller importör att produkten uppfyller EU:s grundläggande hälso-, miljö- och säkerhetskrav, vilket även innebär att produkten kan säljas fritt över nationsgränserna inom EU (Arbetsmiljöverket, 2020). Eftersom produkterna förväntas uppfylla vissa hälso- och säkerhetskrav resulterar det i en högre grad av patientsäkerhet.[9]

Tillverkare är enligt EU (CE-märkning, 2020) själva ansvariga för att tillse att en medicinteknisk produkt uppfyller alla EU-krav som krävs för att de ska kunna CE-märka sina produkter. Tillverkarna avgör om de kan bedöma sin produkt själva utifrån kraven eller om ett oberoende certifieringsorgan behöver involveras. Vem som kontrollerar produkten beror på vilken produktkategori den tillhör och vilken lagstiftning som är tillämplig för produkten. Om produkten inte behöver kontrolleras av ett oberoende organ är det tillverkarens ansvar att kontrollera att produkten uppfyller de tekniska kraven samt att bedöma och dokumentera eventuella risker med att använda produkten (EU, CE-märkning, 2020). När tillverkaren sedan CE-märker produkten upprättar denne också en EU-försäkran som ska finnas tillgänglig ytterligare 10 år efter att produkten har slutat tillverkas (Elsäkerhetsverket, 2017).

[8] CE: Conformité Européenne, produktsäkerhetsmärkning som har lagstadgats av EU.

[9] Under Covid-19-pandemin har ett så kallat snabbspår upprättats av Arbetsmiljöverket på uppdrag av regeringen för att säkerställa ett förfarande för att även icke-CE-märkt personlig utrustning ska kunna användas (A2020/0073/ARM).

2.3.1 Klassning inom CE-märkning

Det finns fyra klasser för CE-märkning av medicintekniska produkter: klass I, IIa, IIb och III. Klassificeringen bygger på vilka risker en patient kan utsättas för på grund av en produkts konstruktion, tillverkningssätt eller användning. Vidare bedöms faktorer som användningstid, om produkten är invasiv eller inte samt om den avger energi till patienten. Bedömningen vid klass I-produkter utförs i regel av tillverkaren och bedömningen av högre klasser utförs i samarbete med ett anmält organ. För klass I försäkrar tillverkaren att produkten uppfyller de väsentliga kraven samt upprättar en teknisk dokumentation och försäkran som bevaras i minst fem år. För klass IIa krävs att bedömningen görs av ett anmält organ ur vissa aspekter. Tillverkaren har möjlighet att välja mellan två alternativ. Det ena alternativet är att tillverkaren själv intygar att produkten uppfyller de väsentliga kraven, där det anmälda organet certifierar och godkänner varje exemplar eller kvalitetssystem för produktion och/eller slutprovning. Det andra alternativet är att låta det anmälda organet bedöma och godkänna tillverkarens totala kvalitetssystem. För klass IIb och klass III har produkter en hög riskpotential vilket innebär att de alltid ska bedömas av ett anmält organ. Tillverkaren kan välja mellan två alternativ: antingen att det anmälda organet bedömer och godkänner tillverkarens totala kvalitetssystem eller att det anmälda organet typprovar produkten samt kontrollerar och godkänner varje exemplar eller kvalitetssystemet för produktion och slutprovning (Banck, 2019).

2.3.2 Bristen på anmälda organ

Det har uppmärksammats en brist på anmälda organ med rätt att certifiera enligt både MDR och IVDR.

I september 2020 fanns i Europeiska kommissionens publika databas Nando[10] knappt 40 anmälda organ i Sverige, varav två för medicintekniska produkter enligt tidigare gällande direktiv (93/42/EEC): RISE och Intertek Semko AB (SOU 2021:19, s. 711).

I höständringsbudgeten för 2020 tillförde regeringen 15 miljoner kronor till RISE för att säkerställa att Sverige också enligt det nya medicintekniska regelverket som började tillämpas i maj 2021 skulle ha ett anmält organ för certifiering av medicintekniska produkter (SOU 2021:19, s. 713). Utredningen menar att förmågan att certifiera produkter även har betydelse för svåra situationer som covid-19 och andra försörjningskriser eller krig.

Branschföreningarna Swedish Medtech, Swedish Labtech och De forskande läkemedelsföretagen (LIF) har i ett brev till tidigare näringsminister Ibrahim Baylan och socialminister Lena Hallengren belyst den oro som finns gällande bristen på anmälda organ. Bristen på anmälda organ anses vara akut och det föreslås att alla

[10] Nando (New Approach Notified and Designated Organisations) (EU-kommissionen, 2021)

produkter som klassas upp (det vill säga får en högre klass) i övergången till IVDR, och därmed behöver ett anmält organ, får förlängd övergångstid (Swedish Medtech, 2021).

I brevet beskrivs att det i dag endast finns fyra tillgängliga anmälda organ för IVDR inom EU, vilka redan nu rapporterar att de inte har kapacitet att ta emot nya kunder. Hälso- och sjukvården inklusive de grupper som företräder sjukhus, anmälda organ, laboratorier och vårdpersonal delar den oro som tillverkare och leverantörer ger uttryck för (Swedish Medtech, 2021).

Flera av de in-vitro-diagnostik-tester som i dag finns på marknaden löper hög risk att inte kunna certifieras i tid enligt de nya kraven. Detta resulterar i att hälso- och sjukvården får brist på en mängd tester som är signifikanta för sjukvården. Samma problem anses finnas för nya innovativa produkter där det kommer att vara problematiskt för företagen att genomföra CE-märkning enligt IVDR i rådande situation. Den pågående pandemin har påverkat förmågan att förbereda sig för IVDR eftersom många anmälda organ hindras från att utföra revisioner på plats, vilket är ett krav för certifiering av in-vitro-diagnostik-tester (Swedish Medtech, 2021).

2.4 Vad säger intervjupersonerna om regelverket?

I det följande redovisas resultat från intervjuerna med representanter för företagen, Läkemedelsverket, RISE och regionerna rörande regelverket.

2.4.1 MDR

Läkemedelsverket är behörig myndighet, utsedd av regeringen, med ansvar för alla de delar som nämns i MDR rörande medicinteknik. Myndigheten har stött på att företag säger att man har sett över sin produktportfölj och att man äntligen kan ta bort produkter som man inte velat ha kvar i sin produktportfölj, men som det funnits en efterfrågan på hos kunderna. Både myndigheter och tillverkare tror att vissa produkter kommer att försvinna. Läkemedelsverket kan inte påverka företagens beslut; de drivs av marknadsintressen. Men myndigheten kan ha en dialog med företagen. Det har hänt att en produkt har behövt dras in från marknaden av säkerhetsskäl och att det tar lång tid innan det kommer ut en ny version (Läkemedelsverket - intervju, 2021).

Enligt RISE har man, i en jämförelse mellan MDD och MDR, gjort framsteg i beskrivningarna. Fler vägledningsdokument kommer också; området är fortfarande ungt. När MDR används av fler kommer det att bli tydligare, och det kommer att finnas mindre möjligheter att tolka regelverket olika. Det gamla regelverket kunde tolkas mer olika. Generellt ställer MDR högre krav på klinisk

utvärdering och teknisk dokumentation. Det viktiga är att man som företag förbereder sitt underlag innan man kommer till det anmälda organet. Man vinner mycket i sin egen tidslinje om man har gjort ett grundligt jobb i förväg (RISE - intervju, 2021).

Om man ska vara certifierad enligt MDR krävs mer resurser än tidigare, både personrelaterade och ekonomiska. Kostnaderna för att göra en bedömning ökar. Hos RISE behövs mer resurser, och det är i slutändan tillverkaren som får betala för det. Då kanske det innebär att man går miste om små innovationer. Samtidigt är syftet att se till att det finns säkra produkter ute hos användarna. Reaktionerna från andra länder om MDR är desamma, att kostnaderna för de små tillverkarna blir så höga, att de antingen köps upp eller att de försvinner. Faran med detta är att det i slutändan bara finns ett tiotal stora aktörer som producerar medicintekniska produkter, vilket kan begränsa framtida möjligheter (RISE - intervju, 2021).

En föreskrift som Läkemedelsverket arbetar med är reglering av nationella medicinska informationssystem. I vården finns det många system som tidigare inte uppfyllde definitionen för en medicinteknisk produkt och därmed var oreglerade. Regionerna vill veta hur det ska regleras för att kunna köpa in lämpliga system (Läkemedelsverket - intervju, 2021).

Läkemedelsverket arbetar med implementeringen av MDR och IVDR, främst genom EU-arbetsgrupper inom medicinteknik. För tillfället finns inte alla lagtexter på plats. Myndigheten arbetar därför med att färdigställa lagtexter och ta fram vägledningsdokument. Det finns en ”roadmap” som beskriver vad som finns kvar att göra. Industrin hade naturligtvis önskat att vägledningsdokumenten redan fanns. Myndigheten har flera personer som arbetar med EU-texterna. Nu med de europeiska förordningarna kommer Läkemedelsverket inte att ta fram några egna nationella vägledningar, utan arbetar för att ta fram de europeiska vägledningarna. För cybersäkerhet har International Medical Device Regulators Forum[11] (IMDRF) tagit fram ett dokument som heter *Principles and Practices for Medical Device Cybersecurity.* Medical Device Coordination Group[12], där Läkemedelsverket ingår, har också tagit fram ett dokument *Cyber security and medical devices 2020* (Läkemedelsverket - intervju, 2021).

2.4.2 CE-märkning

Om det finns en produkt på marknaden som man kan köpa får man inte egentillverka den. Om den produkt som behövs inte finns på marknaden, får den tillverkas förutsatt att den därefter CE-märks. Produkten blir då inte en egentillverkad produkt. Läkemedelsverket anser att IVO måste sprida kunskap om detta så att aktörerna inte ser regelverket som slutet för innovation, utan som en möjlighet.

[11] Består av representanter från hela världen.
[12] En grupp på EU-nivå.

Enligt Läkemedelsverket finns det hos regionerna en oro för att det kommer att kosta pengar, men den som har följt nationell lagstiftning för egentillverkade produkter vet att det har kostat pengar att uppfylla de krav som har ställts tidigare. Om man har gjort något utan att helt ha följt regelverket, kommer man att få problem och det kan bli en problematisk övergång. Utmaningen med övergången är att det inte finns någon möjlighet att stänga ett sjukhus. Om sjukhuset har implementerat en lösning, måste Läkemedelsverket hantera det. (Läkemedelsverket - intervju, 2021)

Enligt en av de intervjuade IT-driftscheferna vid en region anses den stora svårigheten vad gäller medicintekniska system vara att leverantörerna inte kan efterleva de regelverk som finns inom regionen utan att certifieringen för en produkt måste brytas. Att bryta en certifiering skulle innebära att leverantören lämnar över ansvaret för produkten, men enligt IT-driftschefen måste certifieringar brytas om cybersäkerheten ska säkras. Detta problem tros delvis bero på att IT-avdelningen kommer in för sent i upphandlingarna för att vara med och sätta kraven.

2.4.3 Bristen på anmälda organ

Läkemedelsverket är ansvarig myndighet för att utse och kontrollera anmälda organ (Läkemedelsverket, 2021).

RISE hoppas bli godkänt som anmält organ för MDR. RISE påbörjade ansökan om att bli anmält organ 2019, men 2020 togs beslut om att dra tillbaka ansökan. Under hösten samma år togs nytt beslut om att dra igång ansökan igen. RISE anser att Sverige blir sårbart när det inte finns något anmält organ i Sverige, något som har blivit tydligt under pandemin. Branschen (som berörs av MDR) är inte störst, men väldigt kritisk och viktig. RISE har ett uppdrag från staten genom Näringsdepartementet (RISE - intervju, 2021).

För MDR är det enligt RISE otroligt viktigt med oberoendet och opartiskheten. RISE i form av funktionen anmält organ måste kunna visa att man inte har koppling till andra delar i RISE. RISE har därför bildat ett dotterbolag med egen styrelse och VD. Det är en utmaning att skapa det här bolaget och fylla det med kvalificerad personal innan företagens certifikat går ut 2024. Medtech-branschen är en relativt liten bransch. Att bygga upp ett anmält organ kräver mycket resurser innan man får intäkter, så man måste ha en stark finansiell grund (RISE - intervju, 2021).

Det som RISE redan har sett i MDD-arbetet, är att det medicintekniska området är en verksamhet som ökar mycket med alla appar, och utrustningen har fått en omklassificering. Kunskap om appar och deras kod är en del av den kompetens som RISE eftersöker när man anställer, eftersom den kunskapen är otroligt viktig när man granskar (RISE - intervju, 2021).

Företagen som har intervjuats i denna studie har löst sina certifieringar med hjälp av företag från andra länder i Europa. De större företagen har sedan tidigare haft

goda kontakter med ett anmält organ, som de har kunnat fortsätta använda för MDR. Företagen har ändå märkt att det är brist på anmälda organ, vilket de märkt på hur upptagna de anmälda organen är, och de tror att det är tufft för många företag, särskilt de mindre företagen. De själva tycker antingen att de har haft tur eller arbetat aktivt med frågorna sedan länge och därför ligger bra till. De företag som arbetar bland annat på den amerikanska marknaden har länge behövt följa striktare regler i vissa avseenden.

De anmälda organ som de intervjuade företagen använder är TÜV SüD[13] och DNV GL Presafe[14], vilka båda har sina säten utanför Sverige, och är globala aktörer som har arbetat länge med certifiering av medicintekniska produkter.

[13] TÜV SÜD var från början ett tyskt företag som numera arbetar på den globala marknaden med revision, certifiering, granskning och testning (TÜV SüD, 2021).

[14] Presafe (ett tidigare joint venture mellan de globala certifieringsorganen DNV GL Business Assurance och Nemko) ägs av DNV Business Assurance Group, som ägs av stiftelsen Det Norske Veritas (Vestvik-Lunde, 2018).

3 Cybersäkerhet i vården

Vårdens effektivitet och förväntade resultat, patientsäkerheten samt data- och systemsäkerheten är tre nyckelegenskaper i arbetet med riskhantering för medicintekniska IT-nätverk (Svensk standard, SS-EN 80001-1, 2011). Flera av de intervjuade inom medicinteknik i regionerna lyfter detta som grunden för deras risk- och säkerhetsarbete, och kopplar detta till såväl certifiering som avvikelsehantering.

Nedan redogörs för varför patient- cyber och informationssäkerhet är viktiga för medicintekniska produkter, hur informationssäkerhet kommer in i MDR samt vikten av samarbete mellan medicinteknik och IT i arbete med cybersäkerhet.

3.1 Patient-, cyber- och informationssäkerhet

Ur ett cybersäkerhetsperspektiv liknar medicintekniska produkter industriella informations- och styrsystem, och på samma sätt ökar risken att medicintekniska produkter slås ut när de kopplas upp mot Internet (Hedtjärn Swaling & Mossberg Sonnek, 2016). När fler medicintekniska produkter kopplas upp mot Internet, via olika nätverk, uppstår nya sårbarheter och risker för de produkter som tidigare stod för sig själva och inte kommunicerade med omgivningen. Att säkerställa cybersäkerhet blir därför viktigt både för traditionella IT-system och för medicintekniska produkter (Ingemarsdotter, Hedtjärn Swaling, & Eidenskog, 2020).

Medicintekniska produkter består ofta av samma mjukvara och hårdvara som de vanliga kontors-IT-systemen, och styrsystemen inom hälso- och sjukvård är ofta av samma typ som de som används inom industrin (Lindahl, Rikskonferensen Folk och Försvar, 2021). Om en angripare får tillgång till dessa system kan det innebära en fara för patientsäkerheten. Cyberangrepp inom vårdsektorn skulle kunna leda till nedstängningar av ambulansverksamhet eller sjukhus. Anställda inom hälso- och sjukvården kan även övertygas att vidta åtgärder som verkar rimliga, men som endast är ett sätt för angriparen att få tillgång till systemen och göra dessa osäkra (Lindahl, Rikskonferensen Folk och Försvar, 2021). Att en produkt blir utsatt för ett cyberangrepp, exempelvis skadlig kod, kan påverka patientsäkerheten genom att produkten slutar fungera, läcker känslig information eller behöver startas om för att kunna rensa bort den skadliga koden (Eidenskog, 2020). Om ett cyberangrepp innebär att patientsäkerheten i för hög grad påverkas, kan det även innebära att åtgärder för att hantera cyberangreppet inte kan genomföras (Önne, 2020). När en medicinteknisk utrustning är uppkopplad mot interna nätverk eller Internet, är det viktigt att förstå hur riskerna och hoten förändras jämfört med när utrustningen inte är uppkopplad (Önne, 2020).

Under covid-19-pandemin har det från olika håll rapporterats om en ökande mängd cyberattacker där några av dessa har riktats mot aktörer inom vårdsektorn

(Lindahl, Liljedahl, & Waleij, 2020). En typ av attack är så kallade ransomware-attacker[15] som kan orsaka allvarliga avbrott om de genomförs, och som då kan bli kostsamma. Attacker under pandemin ökar även mot andra verksamheter såsom verksamheter inom energi-, vatten- och transportsektorer, och eftersom sjukvården är beroende av dessa verksamheter för sin funktion, påverkar även dessa attacker sjukvården (Lindahl, Liljedahl, & Waleij, 2020).

Att nu även journalsystem och medicintekniska appar omfattas av MDR innebär att informationssäkerheten i dessa system också kan vara viktig för patientsäkerheten. Inspektionen för vård och omsorg (IVO) tittar inte primärt på informationssäkerhet, utan på att regelverket för medicintekniska produkter följs. Men IVO tar med den kompetens som finns internt inom informationssäkerhet när det behövs eftersom det är olika regelverk som ska pusslas ihop. Det kan vara så att IVO efter en tid upptäcker att det rör informationssäkerhetsfrågor i ett ärende, och då kopplas personer med den kompetensen in (IVO - intervju, 2021).

3.2 Cybersäkerhetsarbete

Följande två kapitel redogör för intervjuresultat. De intervjuade regionerna har i varierande omfattning varit utsatta för cyberangrepp. Regionerna står i dag inför ett teknikskifte och en digitalisering, innefattande exempelvis informationsklassning av information i medicintekniska system. Arbetet för att skapa rutiner för cybersäkerhet håller på att utvecklas och regionerna har kommit olika långt. Ett problem som lyfts är otillräcklig finansiering för IT-säkerhetsfrågor.

I en region finns exempelvis en informationssäkerhetsgrupp som arbetar med att rapportera till IT vilken hotbild som kan uppkomma. Samarbeten finns även med några av de större säkerhetsleverantörerna kring utrustning, system och stöd kring extra omvärldsbevakning.

En region menar att IT har ett antal nyckelåtgärder som har varit till stor hjälp för att skydda mot cyberangrepp, men att ett kontinuerligt arbete behövs för att uppdatera skyddet.

Inom vården har det enligt flera regioner tidigare förekommit att system inte har uppdaterats med ursäkten att IT-åtgärder kan äventyra patientsäkerheten. I dag uppkommer dessa protester mer sällan. Detta tror flera av de intervjuade kan förklaras med den generella digitaliseringen i omvärlden, vilken har resulterat i en högre medvetenhet avseende de IT-relaterade utmaningar som finns. I och med utvecklingen avseende digitaliseringen och högre grad av IT i medicintekniska produkter är även samarbetet mellan medicinteknik och IT relevant i cybersäkerhetsarbetet.

[15] Kalix kommun drabbades den 16 december 2021 av en ransomware-attack, som slog ut stora delar av kommunens IT-system, bland annat omsorgen. (https://www.kalix.se/, besökt 2021-12-21.)

Kunskapen avseende cybersäkerhet behöver generellt förbättras. Exempelvis har det identifierats ett behov av att genomföra utbildningar för förvaltningschefer och politiska nämnder inom cybersäkerhet och hotbilder. En region berättar om en sådan utbildning som skulle ha genomförts under 2021, men blev uppskjuten på grund av pandemin.

I en region används en produktdatabas där de medicintekniska produkter som används i regionens nät är registrerade. De produkter som inte finns med i denna databas får heller inte vara anslutna till näten.

Under de månadsvisa servicefönstren så har IT-enheter direktkontakt med de mest akuta verksamheterna som då kan säga stopp till IT att genomföra vissa förändringar.

Generellt bland de tillfrågade anses att det inte går att bygga upp produkter som är helt säkra, utan det blir en kombination av en säker produkt och en säker drift av produkten. Två funktioner som nämns i sammanhanget är att all access och nyttjande av systemen loggas så att man i efterhand kan se vem som varit i systemet och vad som har gjorts. För patientjournaler är detta ett krav på vårdgivarna enligt patientdatalagen (2008:355). Den andra funktionen är ”break the glass”, exempelvis om akuten behöver rättigheten till viss information eller system kan de medvetet göra en sorts override-funktion.

Ett annat exempel som ett av företagen nämner är effektiviteten kontra sekretessen. Att man med en sökfunktion kan söka efter patienter som har någon viss åkomma eller via patient-ID kan leda till problem med patientskyddet om man får en träff, samtidigt som om man inte har sökfunktionen kan få en sämre effektivitet. Företaget jobbar med den balansen och avvägningen.

En ytterligare utmaning som ett företag lyfter är när klagomål på medicintekniska produkter behöver utredas och åtgärdas. Problem med patientsäkerheten får företaget inte kommunicera till vare sig säljare eller användare innan analysen är klar. Företagen får inte heller åtgärda felet innan myndigheterna är underrättade. Men, med cybersäkerhet är det tvärtom. Där måste man när man är medveten om problem publicera detta medan man gör analysen och dela med sig av informationen om potentiella hot. Det behövs en kulturförändring så att detta görs. Cybersäkerheten kan påverka patientsäkerheten så man behöver nya arbetssätt och nya processer både hos företagen och i regionerna.

Regioner upplever det problematiskt att hantera flera olika versioner av en programvara. Ett företag berättar hur de gör när nya uppdateringar släpps av till exempel Microsoft. De testar då dessa uppdateringar mot mjukvaran i den medicintekniska produkten för att se om den påverkas eller inte. Oftast påverkas den inte, och då går det bra att vårdgivarna installerar den senaste uppdateringen.

Medicinteknisk och IT-personal har inte alltid samma syn på cybersäkerhet i medicintekniska produkter, och produkter klassas som att antingen tillhöra IT eller

medicinteknik. Ibland upplever regionerna att det finns en krock mellan cyber- och patientsäkerhetsfrågor, exempelvis som att IT vill införa två-faktor-autentisering medan vårdpersonal har svårt att hinna med en tvåfaktorsautentisering.

Ifall man inte kan garantera cybersäkerheten gentemot andra system, anser flera av de intervjuade regionerna att det enda rätta är att låta utrustningen vara fristående.

En av de intervjuade regionerna upplever att MSB inte i stor utsträckning stödjer mindre organisationer som behöver mer kompetens vid exempelvis cybersäkerhetsincidenter. Regionen menar att MSB skulle kunna ha ett antal upphandlade leverantörer som kan avropas utifrån händelse och behov. Vid större säkerhetsincidenter borde det dessutom finnas en central organisation som kan stötta framför allt de mindre regionerna som inte har lika stort organisatoriskt stöd. Vid större säkerhetsincidenter skulle även säkerhetsleverantörer kunna stötta de mindre regionerna med hanteringen av dessa händelser. Även om det pågår en uppbyggnad nationellt så upplevs det av regionen som att arbetet har långt kvar. En annan region menar samtidigt att MSB:s digitala material fungerar att arbeta med och utgå ifrån gällande riskanalyser inom cybersäkerhet. De anses lättare att förhålla sig till jämfört med ISO-standarder som inte är lika tydliga.

När MDR väl har landat in om några år kommer det i vissa avseenden att vara mycket bättre, tror flera av de medicintekniska personer som intervjuats. Medicinteknikerna tror också att tillverkarna kommer att bättre förstå att det är medicintekniska produkter man tillverkar. Cybersäkerheten kommer då att ha förbättrats, och det blir tydligare att cybersäkerhet också är viktigt för prestandan på produkten.

3.3 Samarbete medicinteknik och IT

Intervjuade representanter för både medicinteknik och IT anser att samarbetet mellan dem är av stor vikt för att både patientsäkerheten och cybersäkerheten ska garanteras, men att det ibland innebär utmaningar att samarbeta över avdelningsgränserna. Enligt IVO handlar det om kunskap och kommunikation (IVO - intervju, 2021).

3.3.1 Om organisation och samverkan

Framgångsfaktorer som har identifierats i regionerna för att öka samarbetet är exempelvis att man behöver medvetandegöra varandra om organisatoriska roller, kompetens och förmåga. Man behöver dessutom spela in varandra vid rätt tillfälle som vid upphandling av medicintekniska produkter. Vidare behöver man jämka ihop förvaltning av IT-system, förvaltning av medicinteknisk utrustning och vårdverksamhet.

I vissa regioner finns det konflikter mellan de båda sidorna, men då gäller det enligt de intervjuade att hitta en gyllene medelväg. En del regioner har flyttat in medicinteknik och IT under samma tak, vilket kan underlätta verksamheten. Ledningarna har stort ansvar att allt trillar ner i organisationerna. Det finns ofta isolerade öar som har kunskap, men som inte känner till varandra.

Inspektionen för vård och omsorg anser att det till stor del är en kommunikationsfråga och att det behövs bättre kommunikation mellan medicintekniska avdelningar och IT-avdelningar (IVO - intervju, 2021).

Under de senaste två till tre åren har medicintekniska avdelningar utvecklats och blivit mer involverade med IT. Det är dock av betydelse för flera av regionerna att medicinteknik och IT samverkar i större utsträckning över organisationsgränserna. Det är viktigt för att det är väldigt olika kompetenser som behövs. Ofta är medicinteknikerna också närmare vården än IT. På avdelningar som har mer teknik och system är uppfattningen att det oftast fungerar bättre eftersom medicinteknik och IT där arbetar närmare varandra och samverkar mer. Dock behöver det inte vara så överallt.

Det kan vara problematiskt för de medicintekniska avdelningarna när IT vill göra uppdateringar som kan göra att produkter inte kan användas. Samtidigt tycker representanter för IT-avdelningarna att en medicinteknisk avdelning är tungrodd som vill behålla gammal utrustning.

Hur arbetet med cyber- och patientsäkerhet berör de medicintekniska avdelningarna varierar. I en region fungerar samarbetet relativt bra eftersom den medicintekniska personalen vet vem de kan prata med på IT-avdelningen. IT-funktionen hos en region menar att de inte arbetar med patientsäkerhet mer än att de blir berörda av det via patientnära IT-utrustning. Där finns stöd av medicintekniker vad gäller denna utrustning för att patientsäkerheten och säkerhetskraven uppfylls. Direktkontakt med vårdpersonalen vad gäller IT-frågor finns också, exempelvis vid incidenter. IT informerar dock inte om patientsäkerhet, utan detta sker i andra kanaler.

3.3.2 Om kunskap

Regionernas företrädare är överens om att kompetensen kring cybersäkerhet skulle kunna höjas hos medicintekniska avdelningar, framför allt kring vilka skyddsåtgärder som kan behöva vidtas. Detta bör ske för att skapa ett så bra grundskydd som möjligt. En region vill dessutom att en internutbildning om medicinteknik påbörjas för IT-personal. Denna behövs för att utbilda i varför vissa åtgärder inte kan genomföras i IT-miljön på grund av patientsäkerheten. Pandemin har i en del avseenden försvårat arbetet mellan medicinteknik och IT, men i många fall har också de som initialt arbetade med att ställa om verksamheten under pandemin haft ett tätare samarbete vilket anses ha förbättrat samarbetet generellt mellan medicinteknik och IT.

Ett exempel på denna typ av samarbete lyfts, där verksamheten, medicinteknik, IT och fastighet undersökte om det gick att använda kameraövervakning för att läkarna skulle slippa behöva byta om mellan olika patientkontakter. Projektet implementerades inte men det berodde på andra saker än tekniken.

Flera av de intervjuade vid regionerna lyfter att medicintekniker inte har tillräcklig kunskap om IT, och att IT inte har tillräcklig kunskap om medicintekniska frågor och patientsäkerhetsfrågor men att kunskapen börjar bli bättre. Det viktigaste för medicinteknikerna är att hitta kontaktytor mot IT, men det är inte helt lätt att hitta den kompetensen: någon som har kunskap om både patient- och cybersäkerhet. Medicintekniska avdelningar är ofta inte på samma hierarkiska nivå som IT. IT finns ofta på koncern- eller regionnivå sedan en längre tid, men medicinteknik i de större regionerna håller på att komma upp på den nivån bland annat med syfte att ena medicinteknik och IT.

3.3.3 Om upphandling

I regionerna upplevs det finnas en upphandlingsproblematik då olika perspektiv missas av både medicintekniska avdelningar och IT-avdelningar. En framgångsfaktor för cybersäkerheten är att både medicinteknik och IT kommer in tidigt i kravställningsarbetet i en upphandling. Detta handlar om att säkerställa att produkterna kan användas på de operativsystem som finns. Om det är ny IT-utrustning, är det viktigt att IT är med vid installationen så att en egen certifiering kan göras från IT-sidan.

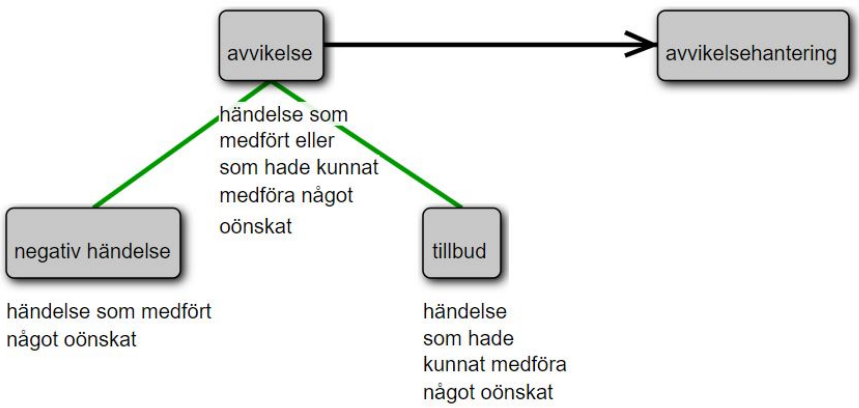
Det förekommer enligt en region fortfarande att det köps in IT-beroende medicintekniska system där IT inte är involverade, men det händer alltmer sällan. Tidigare fanns det i de större regionerna flera olika medicintekniska avdelningar och olika IT-avdelningar i organisationen. Dessa håller på att centraliseras, vilket underlättar samordningen mellan medicinteknik och IT.

IT-avdelningarna deltar ofta i upphandlingar för att ta fram den tekniska kravprofilen för de medicintekniska produkterna och bistår i processen. Även detta är under förändring i flera regioner. Verksamheten köper i dag in och äger i många fall utrustningen, men uppdraget kommer nog förändras så att IT i stället ska äga utrustningen och medicinteknik hålla ihop produktfloran. Medicinteknik eller IT försöker rikta den och skapa bättre säkerhet.

När medicintekniska produkter ska upphandlas, görs en auktoriseringsansökan till IT i flera regioner. IT blir på så sätt inblandade när det gäller inköp av medicintekniska produkter. IT kommer dock ofta in efter beslutet är fattat och avtalet skrivet. Detta är något som IT-avdelningar i många regioner försöker ändra på, så att de ska få vara en del av processen mycket tidigare. Medicinteknik och IT försöker hitta gemensamma grunder att stå på i upphandlingsfrågor. På samma sätt som medicinteknisk kompetens är en resurs i upphandlingar så är IT och informationssäkerhet med och stöttar med upphandlingskrav och liknande.

4 Avvikelsehantering

Det är av betydelse att säkerställa att medicintekniska produkter är säkra och har hög prestanda. För att göra det, är det viktigt att utreda varför negativa händelser och tillbud inträffar. Uttrycket avvikelse används när man rapporterar eller utreder antingen en negativ händelse eller ett tillbud (Socialstyrelsens termbank, 2020). (Se figur 1.) Det är också viktigt att andra användare av likadana produkter kan ta del av vad som har inträffat, för att kunna förebygga att det inträffar i deras organisationer. Att kunna rapportera om och åtgärda felaktigheten så att den inte inträffar igen är därför av yttersta vikt (Holmgren, 2020) och (Ylvén, 2020). Ändringar i och med MDR, som kan komma att påverka hur man hanterar och rapporterar händelser eller tillbud, är bland andra skärpta krav på tillverkarnas kvalitetssystem och riskhanteringsprocesser, vilka förutsätter att hälso- och sjukvården, användarna och tillverkarna har fungerande informationssystem (Mårtensson, 2019).



Figur 1. Förklaring av avvikelsehantering (Socialstyrelsens termbank, 2020, egen modifiering).

I Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården (HSLF-FS 2021:52) står i 5 kap. att om en negativ händelse eller ett tillbud har inträffat med en medicinteknisk produkt, ska en utredning snarast inledas. Anmälan om negativa händelser och tillbud med medicintekniska produkter som inte är egentillverkade ska göras till Läkemedelsverket och tillverkaren. Anmälan som gäller egentillverkade produkter ska göras till Inspektionen för vård och omsorg. Utredningen, bedömningen och vidtagna åtgärder ska, enligt föreskrifterna, dokumenteras.

Dokumentationen kan förutom till myndigheten och tillverkaren göras i olika typer av avvikelsehanteringssystem. Det finns en nationell avvikelsehanteringsdatabas reidarMTP och flera regionala system. Tillverkare rapporterar till den europeiska databasen EUDAMED. Nedan beskrivs EUDAMED och reidarMTP mer ingående samt avvikelsehantering och dess rapportering.

4.1 EUDAMED

EUDAMED är ett IT-system och en databas som följer utifrån implementeringen av EU-förordningarna MDR och IVDR. Syftet med systemet är att öka transparensen och spridningen av information om medicintekniska produkter och system inom EU:s öppna marknad. Sedan tidigare finns en befintlig databas i mindre format under MDD, men som nu byts ut och utökas i samband med MDR och IVDR (EU-kommissionen, 2021).

EUDAMED ska agera som en plattform med information om olika etablerade och certifierade aktörer inom medicinteknik. Till EUDAMED ska tillverkare rapportera olyckor, tillbud och säkerhetsinformation. De övervakande myndigheterna i EU ska ha full tillgång till databasen för att kunna utbyta information, och skapa effektivare system. Databasen kommer dock att innebära en ökad administrativ börda för bland andra ansvariga tillverkare (Mårtensson, 2019). Den nya databasen kommer att ha flera funktioner och vara uppbyggd av sex moduler. Systemet kommer att innefatta en registreringsfunktion samt notifikations-, samarbets- och spridningssystem, som är tillgängligt för allmänheten och aktörerna inom branschen (EU-kommissionen, 2021). Den första modulen släpptes i december 2020, och de resterande modulerna kommer släppas kontinuerligt (MedTech Europe, 2020). Det slutliga systemet ska finnas tillgängligt i maj 2022 i samband med implementeringen av IVDR (Swedish MedTech, 2019).

I avsnitt 4.2 beskrivs hur den öppna nationella avvikelsedatabasen reidarMTP synes fylla en viktig funktion. Hur pass öppet EUDAMED kommer att vara för vårdgivarna och vilken betydelse som systemet kan få för dem ur ett avvikelseperspektiv återstår att se.

Sverige är enligt Läkemedelsverket ett för litet land för att kunna föra bra statistik över avvikelser som rör medicintekniska produkter. Förhoppningen är att det är fler som kommer att rapportera och att det därmed blir bättre översikt med EUDAMED. För tillverkarna blir det enklare med ett system. Ifall Sverige berörs, kommer Läkemedelsverket att meddelas. Myndigheten måste därför utveckla de nationella IT-systemen så att den kan kommunicera med EUDAMED. Förhoppningen är att den nytta som man i dag ser med reidarMTP, att ge snabb information till många, kommer att finnas i EUDAMED. Men EUDAMED blir inte lika detaljerad som reidarMTP (Läkemedelsverket - intervju, 2021).

EUDAMED är ett försök att samordna alla databaser till en enda. Det finns en stor önskan om en portal till vilken man rapporterar, och så skulle systemet sedan skicka rapporten vidare till rätt myndighet. I och med att vi är decentraliserade lägger vi emellertid också ansvaret på användaren att sköta samordningen (Läkemedelsverket - intervju, 2021).

4.2 reidarMTP

Ledningsnätverket för Medicinsk Teknik (LfMT) och Svensk Användarförening för Medicinsk Teknik och IT (SAMTIT) driver tillsammans den nationella avvikelsedatabasen reidarMTP. reidarMTP är ett verktyg som hjälper regioner att få kännedom om eventuella felaktigheter i olika medicintekniska produkter. Genom att avvikelser rapporteras i databasen sprids informationen till regionerna som då kan förebygga att samma avvikelser sker i deras produkter. Då kan regionerna även se om avvikelsen har skett i endast en enstaka produkt eller om det är ett utbrett problem (Ylvén, 2020).

Avvikelserna rapporteras in i reidarMTP utifrån exempelvis typ av händelse, hur allvarlig händelsen var eller hade kunnat bli och vilka situationer som är utsatta för avvikelser. I mars 2018 gjordes en större uppdatering av reidarMTP, och databasen fick då en automatisk koppling till det nationella benämningsregistret MTPreg[16]. Det blev då också möjligt att avpublicera ett ärende och att abonnera på exempelvis rapporter av nya avvikelser (Holmgren, 2020).

reidarMTP är en frivillig databas för att rapportera avvikelser. Alla som rapporterar in till reidarMTP är certifierade rapportörer; 99 % av dessa är sjukhusingenjörer eller medicintekniker och 1 % består av övrig vårdpersonal (Holmgren, 2020).

Analyser av avvikelserna görs för årlig statistik av medicintekniska chefer och blir en erfarenhetsbas för bugghantering och mjukvaruuppdatering. Rapporterna i reidarMTP är avidentifierade med avseende på sjukvårdsorganisationer och individer, vilket försvårar spårning av enskilda avvikelser. Även den som är rapportör till den enskilda avvikelsen är avidentifierad. Att undersöka orsakerna till avvikelserna djupare än med hjälp av sökningarna i reidarMTP förutsätter därför att kontakt tas med någon av de personer som administrerar databasen, att den personen i sin tur tar fram vem som har rapporterat avvikelsen och kontaktar denne för att fråga om det finns mer information som kan delges (Holmgren, 2020). Det finns alltså potential att förenkla möjligheterna att analysera avvikelserna i databasen för att få ut mer information om orsaker och åtgärder.

Som resultaten från 2020 års delrapport om avvikelserapporteringen visar har det skett en markant minskning av antalet rapporterade avvikelser till reidarMTP un-

[16] MTPreg är ett nationellt register över medicintekniska produkter som brukas vid svenska sjukhus.

der de senaste 15 åren. Under 2005 och 2006 rapporterades totalt 340 avvikelser, vilket kan jämföras med totalt 371 rapporterade avvikelser under perioden 2015-2020. Se *Bilaga 4. Avvikelsestatistik*.

4.3 Avvikelserapportering ur regionernas perspektiv

Vid sidan av reidarMTP har samtliga av de regioner som har intervjuats uppgett att de har egna regionala avvikelsehanteringssystem för regionens verksamheter och funktioner. I dessa system rapporteras generellt en bred flora av avvikelser inom regionen som helhet, allt från exempelvis arbetsmiljö till säkerhetsärenden. Rapporteringsfrekvensen av avvikelser till de regionala systemen uppges av flera intervjuade vara något högre än för reidarMTP. Därtill verkar pandemin haft en ytterligare negativ inverkan på rapporteringsfrekvensen för just reidarMTP (Holmgren, 2020). Ofta är det sjukvårdens medarbetare som registrerar avvikelser som de kommer i kontakt med i sitt arbete. Systemen hanterar med andra ord långt fler avvikelser än sådana som enbart rör medicintekniska produkter. En av de intervjuade medicintekniska funktionerna uppger att de rapporterar in leverantörsavvikelser och leveransavvikelser till det regionala systemet. En annan medicinteknisk funktion uppger att det regionala systemet har en ruta som kan kryssas för om en avvikelse rör en medicinteknisk produkt. Den medicintekniska avdelningen får då i uppgift att utreda avvikelsen och dess orsak.

Som framkommit i intervjustudien har de regionala systemen inte alltid initialt utformats för att hantera avvikelser för medicintekniska produkter. Systemen har istället anpassats vartefter för att inkludera medicintekniska produkter, ibland med mindre optimala resultat – systemet är ”jättebra för diariet, har sin funktion, men är inte så bra som avvikelsehanteringssystem i verksamhet med hög belastning” enligt en region. Vid en av de intervjuade regionerna har den medicintekniska funktionen istället skapat en egen, mer informell, procedur för avvikelsehantering som rör medicintekniska produkter. Likaså har det framkommit att IT-funktionen i en region kan ha ett eget separat ärendehanteringssystem för registrering av IT-relaterade avvikelser.

Det finns vissa skillnader i vilken information som rapporteras in om en avvikelse till reidarMTP respektive till de regionala avvikelsehanteringssystemen. Exempelvis uppges att detaljeringsgraden kan skilja sig mellan systemen, där de regionala systemen kan ha ett mer allmänt, bredare fokus, och reidarMTP kan vara mer tekniskt fokuserat. Samtidigt bygger avvikelserapporteringarna till respektive system på samma händelseförloppsbeskrivning och utredning av avvikelsen. Parallell inrapportering av avvikelser till regionens eget system och till reidarMTP innebär därmed till del en dubbelrapportering.

I Region Skåne fanns tidigare en automatisk koppling mellan det regionala systemet och reidarMTP, där relevant information kunde föras över från det regionala systemet till reidarMTP med en knapptryckning. Denna koppling är i dag inte längre möjlig, men försök görs för att införa en automatisk koppling mellan regionala system och reidarMTP för att öka antalet inrapporteringar (Holmgren, 2020).

Läkemedelsverket har ett eget register, med de anmälningar som enligt regelverket ska gå dit. Dock rapporteras inte alla händelser dit heller. Ibland är det efter att leverantören har uppmärksammat ett fel som Läkemedelsverket får vetskap om detta (Holmgren, 2020). Läkemedelsverkets register är heller inte öppet för vårdgivarna att ta del av. Här uppger de intervjuade att reidarMTP fyller en viktig funktion eftersom databasen utgör en del av medicinteknikernas omvärldsbevakning. Med reidarMTP kan de medicintekniskt ansvariga snabbt ta del av inträffade händelser och själva vidta åtgärder för utrustning i den egna verksamheten innan de själva drabbas. Öppenheten är här en stor fördel med systemet.

Av alla avvikelser som sker i vården är det bara en liten del som är relaterade till medicintekniska produkter. Med reidarMTP snabbas möjligheten på att få kunskap om bristande eller potentiellt farlig utrustning, istället för att invänta bestämmelser kring den. Enligt EU ska tillverkaren själv göra en utredning vilket enligt regionerna kan innebära att det går år innan de kan konstatera någon slutsats. Med reidarMTP kan istället informationen snabbt spridas. Som en respondent från en IT-funktion i en region uttryckte det är leverantörer ”ofta försiktiga med att meddela sina andra kunder när svagheter i produkter har uppmärksammats”, något som kanske kan härledas till att det finns PR-relaterade aspekter som leverantörerna vill undvika. Samme respondent uppgav också att man från regionens sida försökt framhålla för leverantörerna vikten av att de också meddelar andra regioner som använder deras produkter när brister upptäcks, dock utan någon nämnvärd respons från leverantörerna.

Den sammantagna bilden från regionernas respondenter är att ett nationellt system för rapportering av avvikelser som rör medicintekniska produkter behövs. Nyttan av systemet bygger dock på att avvikelser faktiskt rapporteras in av de certifierade rapportörerna.

4.4 Avvikelserapportering ur myndigheternas och anmälda organens perspektiv

Vårdgivare är ansvariga för att rapportera oönskade händelser och tillbud. Som vårdgivare är man skyldig att rapportera till flera myndigheter, och det finns inget gemensamt system. På Läkemedelsverket har man lanserat en e-tjänst så att vårdgivarna kan rapportera elektroniskt på ett säkert sätt. Myndigheten har följt statistik över rapporteringen de senaste åren och den har ökat. Man vet inte om det

beror på att vårdgivarna blivit bättre på att rapportera, eller om det beror på att användningen av medicintekniska produkter har ökat (Läkemedelsverket - intervju, 2021).

Enligt Läkemedelsverket producerar tillverkarna system och produkter som kan ha koppling till överföring av trådlösa data och cybersäkerhet. Frågan är om tillverkarna tänker på kontexten, att vårdsystem kan skilja sig mellan länder och att vård bedrivs på olika sätt. Läkemedelsverket har dialog med enskilda tillverkare när det sker olyckor och tillbud och träffar branschorganisationer. Myndigheten måste hjälpa vårdgivarna och tillverkarna att ha en dialog, eftersom MDR pekar ut att vården måste ha ett system för att återkoppla erfarenheterna från användningen till tillverkarna. Det har tillkommit med MDR. Det är huvudsakligen tillverkare och vårdgivare som rapporterar. Vid problem kontaktar vårdgivare tillverkare eller leverantör, som ska åtgärda om något har inträffat (Läkemedelsverket - intervju, 2021).

Läkemedelsverket har inte tillstånd att utöva tillsyn över cybersäkerhetsfrågor i allmänhet, enbart om det finns koppling till patientsäkerhet. Om en patient hade kunnat komma till skada så är myndigheten involverad. Då ser myndigheten till att tillverkaren undersöker hur det kunde hända. Genom rapportering har det exempelvis kommit till kännedom att insulinpumpar haft säkerhetsluckor, att de skulle ha kunnat hackas. Sådana saker har kommit till myndighetens kännedom genom rapportering (Läkemedelsverket - intervju, 2021).

Det är endast frågor som rör patientsäkerhet som hamnar på Läkemedelsverkets bord, och ibland är cybersäkerhet inkluderat. Det är på patientsäkerhetsområdet som myndigheten har mandat att agera, om de ser att en patient kan skadas fysiskt (Läkemedelsverket - intervju, 2021).

Nätverksproblem och IT-utrustning kan orsaka störningar på medicintekniska produkter. Det kan ibland vara svårt att bedöma om det är ett produktfel eller om det kan handla om till exempel sjukhusens kapacitet för nätverk eller el. Det kan vara en mjukvaruuppdatering som görs och som får konsekvenser för en produkt som är beroende av mjukvaran. Gasanläggningar klassas som egentillverkade system och kontrolleras av IVO (Läkemedelsverket - intervju, 2021).

För enskilda produkter kan Läkemedelsverket kräva att produkten dras tillbaka från marknaden eller vidareutvecklas. Ser man större systematiska problem inom branschen så kan myndigheten lobba för lagändringar. Inom EU så handlar det om att kräva förtydligande gällande vägledningar och lagstiftningsändringar. Det är en längre process (Läkemedelsverket - intervju, 2021).

Läkemedelsverket har sett att det ibland är med fel med systemen, men man kan inte stänga ner ett sjukhus. Läkemedelsverkets påtryckningsmedel blir istället att man vill

se en handlingsplan, hur vårdgivaren hanterar problemet (Läkemedelsverket - intervju, 2021).

Läkemedelsverket ger återkoppling enskilt till den som rapporterat. Våren 2021 skedde en incident med en sterilanläggning som inte fick användas. Händelsen ledde till krisberedskapsmöten där Läkemedelsverket samverkade med vårdgivare. Regionerna fick berätta om de hade denna utrustning eller inte, och man lånade av varandra för att klara krisen. Enligt Läkemedelsverket visar denna händelse att man måste ha koll. Kan detta drabba min region? Finns det alternativa produkter? Läkemedelsverket anser att fler behöver rapportera avvikelser och förstå nyttan med rapporteringen. Om alla i EU är i samma modul i EUDAMED ska man kunna se totala antalet incidenter (Läkemedelsverket - intervju, 2021).

Enligt Läkemedelsverket prioriterar vårdgivarna de legala rapporterna i första hand. reidarMTP är otroligt detaljerad, och det är ett problem om vårdgivarna inte har tid att göra sina rapporteringar (Läkemedelsverket - intervju, 2021).

Enligt RISE finns det en skyldighet för tillverkare att rapportera, men om det ska vara till någon nytta så måste andra kunna ta del av informationen. Det måste vara tydligt för andra som läser, eftersom syftet är att hjälpa andra att undvika att drabbas. Avvikelserapporteringen kan även användas i upphandlingar. RISE anser att rapporteringen från användarna är otroligt viktig. Med EUDAMED kanske det kommer bli bättre, eftersom andra kan komma in och läsa där. Men till EUDAMED rapporterar enbart tillverkarna (RISE - intervju, 2021).

RISE utför revisioner hos tillverkarna, och tittar på avvikelsehantering. Det är generellt svårt att få till avvikelsehanteringen så att det blir en rapport av det. Man ska göra så många delar i en avvikelserapportering, någon ska rapportera och sedan ska det analyseras, grundorsaksanalys, korrigerande åtgärder etc. Men man hinner inte riktigt sätta sig ner och fundera över grundorsaken, så att man slipper hamna i samma sits igen och igen (RISE - intervju, 2021).

4.5 Orsaker till utebliven rapportering

I 2020 års NCS3-studie (Eckersand & Wahrenberg, 2021) om inrapporteringen av avvikelser till reidarMTP konstaterades att rapporteringsfrekvensen kontinuerligt sjunkit under 2000-talet (se *Bilaga 4. Avvikelsestatistik*). Detta skedde från en nivå som förmodligen redan från början bara utgjorde en mindre del av alla de avvikelser som faktiskt har skett i verksamheterna. Frågan är vad som kan vara anledningarna till att det uppges ske en allmän underrapportering till reidarMTP. I det här avsnittet redogörs för de orsaker som har framkommit i samband med studiens intervjuer.

4.5.1 reidarMTP används bara av certifierade rapportörer

Rapportering av avvikelser till reidarMTP görs endast av certifierade rapportörer, vilka tillhör LfMt som är de medicintekniska chefernas nätverk. De certifierade rapportörerna finns därmed bara på de medicintekniska enheterna vilket innebär att endast en delmängd av alla som använder medicintekniska produkter inkluderas. Rapporteringen blir därmed sned då avvikelser med exempelvis medicintekniska produkter på hjälpmedelscentraler, laboratorier, syn- och hörselcentraler eller i tandvården inte inkluderas. Även fel med produkter som finns i gränslandet mot IT som exempelvis journalsystem och appar samt förbruknings- och engångsmaterial som sprutor är uteslutna från reidarMTP. Detta kan också förklara varför det inte rapporteras in särskilt många IT-relaterade händelser till reidarMTP (Ylvén, 2020). Inrapporteringen till reidarMTP har också visat sig vara personberoende och beror även på vilken organisation rapportören tillhör (Holmgren, 2020).

4.5.2 Osäkerhet i ansvarsfördelning

Det kan finnas osäkerheter i regionerna om vem som ska rapportera inträffade avvikelser. Enligt Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården (HSLF-FS 2021:52) ska vårdgivaren utse och dokumentera vem i personalen som ska vara anmälningsansvarig. Det kan också finnas osäkerheter kring vem som åtgärdar en avvikelse. Om till exempel den anmälningsansvarige endast felanmäler produkten och inväntar att produkten ska bli åtgärdad i tron att någon annan rapporterar avvikelsen, riskerar avvikelsen att inte rapporteras. På en del sjukhus är det de medicintekniska cheferna som har ansvaret att rapportera, men de har inte tillgång till alla produkter eftersom en del finns ute i verksamheterna. IT har inget uppdrag att rapportera medicintekniska avvikelser, men hanterar en del produkter som kan kategoriseras som medicintekniska. Ingen aktör inom hälso- och sjukvården har alltså helhetsperspektivet över vem det är som ska rapportera. Ju fler system som regionen har att förhålla sig till, desto svårare blir det (Ylvén, 2020).

4.5.3 Olika syn på vad som är en avvikelse

På Sahlgrenska sjukhuset rapporteras ungefär 1 000 avvikelser varje år i den regionala databasen och enligt den intervjuade riskhanteringssamordnaren rör 10-20 % av dessa avvikelser medicintekniska produkter och skulle behöva rapporteras in till reidarMTP. Resterande avvikelser har inte med de medicintekniska produkterna att göra. Inrapportering av en avvikelse per vecka anses som ett rimligt antal, men i nuläget rapporteras uppskattningsvis ca 25 avvikelser per år (Ylvén, 2020).

Det är dock inte alltid själva inrapporteringen som skapar svårigheter i den aktuella regionen. Ibland rapporteras avvikelser in till den regionala databasen som IT-avdelningen tar del av och IT-avdelningen åtgärdar därefter snabbt felet. IT-avdelningen uppges i dessa fall sällan ha undersökt varför avvikelsen uppstod.

Detta tror riskhanteringssamordnaren beror på tolkningen av vad avvikelserapportering är eftersom en avvikelse inte alltid betyder samma sak för vården som för IT-tekniker (Ylvén, 2020). Avdelningarna som ansvarar för medicinteknik och IT samarbetar sällan och har olika fokus, där vården och medicinteknikerna fokuserar på patientsäkerheten och IT på att främst åtgärda uppkomna fel i systemen (Önne, 2020). Exempelvis bedöms enligt riskhanteringssamordnaren en felaktigt larmande maskin som en avvikelse inom vården eftersom detta påverkar patientsäkerheten. Eftersom det inte behöver vara fel på utrustningen, bedömer ofta inte IT-teknikerna det som en avvikelse. IT-teknikerna identifierar fel i utrustningen som avvikelser. Dessutom är det vanligt att IT-personal tolkar avvikelsehantering som avhjälpande åtgärder vid driftstopp, inte utredning och rapportering av negativa händelser och tillbud, medan medicinteknisk personal i avvikelsehantering även inkluderar utredning och rapportering (Ylvén, 2020).

4.5.4 Rapportering prioriteras inte

Till skillnad mot den obligatoriska avvikelserapportering som ska ske till myndigheter och tillverkare samt till regionens egna regionala system är avvikelserapporteringen till reidarMTP en frivillig uppgift. Som framkommit i denna intervjustudie är det enligt regionerna med andra ord inte reidarMTP som prioriteras av användarna om tiden är knapp. Även för de regionala systemen uppges det finnas utmaningar. Framför allt finns det utmaningar i verksamheter som är hårt belastade såsom akuten eller intensiven. Där är det ont om tid för exempelvis IVA-sköterskorna att prioritera avvikelserapportering. Speciellt svårt är det om rapporteringsverktyget är krävande, inte användarvänligt eller personalen inte förtrogen med verktyget.

Den ökade belastning som pandemin har medfört för vården tycks enligt regionerna ha bidragit till en ytterligare minskning av rapporterade avvikelser. Fokus för den medicintekniska avdelningen har framför allt legat på att se till att vården har haft de produkter som har behövts, inte på att utreda avvikelser. Därtill uppges att cheferna inte alltid har gett tillräckligt med utrymme för att ägna sig åt avvikelserapportering. Dessutom har de prioriteringar som vården har behövt göra under pandemin också lett till att det varit svårare för medicinteknikerna att få tag på det folk som behövs för att kunna genomföra en utredning, vilket kan ta upp till dagar eller till och med veckor.

4.6 Rapportering av IT-relaterade avvikelser

Det finns flera möjliga förklaringar till varför få IT-relaterade avvikelser rapporteras in till reidarMTP. En skulle kunna vara att det helt enkelt inte sker särskilt många IT-relaterade incidenter inom vården. Att det förekommer angreppsförsök eller rekognosering mot vårdens olika produkter och system som är exponerade mot internet står dock klart. Men med ändamålsenliga skydd har det

i intervjustudien också framkommit att intrångsförsök hittills har kunnat hindras och att det därför inte i flera regioner har förekommit några incidenter att rapportera. I ett annat fall uppges att det årligen förekommer mellan 100 och 200 informationssäkerhetsincidenter inom regionen, men att man vid informationssäkerhetsfunktionen inte har hanterat en enda incident som rört medicintekniska produkter och system under de senaste två åren. I kontrast till dessa bilder vittnar en tredje respondent, som också arbetar vid IT-funktionen hos en region, att det allmänt sker en ökning över tid vad gäller incidenter, att många applikationer som används i regel är gamla och att hotbilden hela tiden ökar.

De som rapporterar in avvikelser till reidarMTP är certifierade rapportörer som enbart återfinns på de medicintekniska enheterna. Det betyder att det finns medicintekniska produkter i regionerna som dessa personer inte arbetar med, och som de då heller inte rapporterar in några potentiella IT-relaterade avvikelser för. Även om en IT-incident skulle drabba en medicinteknisk produkt som de certifierade rapportörerna får kännedom om är det dock inte säkert att avvikelsen för den skull skulle rapporteras in till reidarMTP. Som en respondent från en medicinteknisk avdelning uttryckte det har de inte betraktat reidarMTP som ett system för cyberrelaterade händelser och har av den anledningen inte heller rapporterat sådana dit. Fokus har legat på att rapportera avvikelser som rör själva produkten eller systemet och fel däri. Respondenten ser förvisso inga problem med att börja rapportera cyberrelaterade incidenter, men eftersöker i så fall tydliga riktlinjer för den typen av rapportering, exempelvis från LfMt, som också behöver understryka vikten av att rapportering sker.

Datorrelaterade medicintekniska produkter kan delas upp i kategorier efter vem som sköter driften. Administrativa datormiljöer med vanliga operativsystem såsom Windows sköts oftast av regionernas IT-enheter medan driften av operativa produkter med egna inbäddade operativsystem och mjukvaror sköts i vårdmiljöerna av den medicintekniska personalen eller av leverantörerna av produkterna (Holm & Westring, 2015). Det finns också system som berör såväl medicinteknisk personal som IT-personal, där dessa båda personalkategorier behöver kommunicera med varandra (Ylvén, 2020). I LfMt:s vägledning för avvikelsehantering beskrivs att det i dag finns brister i samarbetet kring avvikelsehantering vilka leder till att vissa typer av avvikelser och produktområden inte utreds eller rapporteras (LfMt, 2018). Att det behövs ett samarbete mellan medicinteknik och IT för hantering av avvikelser med medicinska informationssystem lyfts här fram som ett exempel.

Även i intervjustudien framkommer att det finns en uppdelning av ansvaret för medicintekniska produkter mellan medicinteknik och IT. Exempelvis görs i regionerna en bedömning vid installationsfasen av vad det är för typ av utrustning och om utrustningen är en medicinteknisk produkt eller en IT-produkt. Ansvaret för att göra en utredning vid en avvikelse hamnar därmed på den som äger utrustningen. IT-relaterade händelser anmäls normalt till regionens IT-support. För IT-

supporten kan det dock vara så att det inte är lika naturligt att tänka att händelsen också ska rapporteras in som en händelse i regionens avvikelsehanteringssystem, det vill säga utöver IT-funktionens eget ärendehanteringssystem. Om det är IT-funktionen som upptäcker och utreder en avvikelse kommer den därmed sannolikt inte heller att rapporteras in i reidarMTP. Enligt en medicinteknisk respondent förekommer det avvikelser som rapporteras till IT-funktionen som är så pass allvarliga att de borde rapporteras till Läkemedelsverket. Från IT-håll uppges att rapportering sker i enlighet med NIS-direktivet[17] om avvikelsen är så pass allvarlig att den uppfyller kraven för det.

Som ett led i att öka antalet rapporterade cybersäkerhetsrelaterade avvikelser behöver regionerna fundera över vilken rapportering som måste göras. Ärenden ska ibland rapporteras till flera myndigheter. Som exempel kan nämnas att en cybersäkerhetsincident med en medicinteknisk produkt som dessutom genererar strålning, ska rapporteras till Läkemedelsverket, tillverkaren, IVO (utifrån NIS-direktivet) och Strålsäkerhetsmyndigheten. Om incidenten ska Lex Maria-anmälas så blir det dessutom en rapport till IVO. Vid Sahlgrenska Universitetssjukhuset försöker man att göra en och samma utredning för samtliga rapporteringar (Ylvén, 2020). Detta är ett tankesätt som Ylvén uppger behöver införas i större grad för hela regionen. En utredning, men flera rapporter.

En ytterligare åtgärd som lyfts fram av regionerna för att öka rapporteringen av IT-relaterade avvikelser, till de regionala systemen liksom till reidarMTP, är att tydliggöra att IT-funktionen är en del av vårdgivarens organisation. Förbättrade ledningssystem kan behövas för att tydliggöra vem som har ansvar att rapportera avvikelser. I det här sammanhanget uppges de nya regelverken (MDR/IVDR) kunna vara till stöd.

4.7 Förslag för förbättrad avvikelserapportering

I intervjuerna av regionernas företrädare har flera funderingar och förslag framkommit på hur inrapportering av avvikelser kan förbättras, både till de regionala systemen och till reidarMTP. Att en avvikelse registreras i ett system bygger på att någon upptäcker den och sedan väljer att rapportera den. Som en respondent uttryckte det är denna initiala del den viktigaste men också den svåraste – hur man får folk att rapportera avvikelser. Processen att rapportera avvikelser måste vara enkel. Oavsett verktyg och system så är det svårt att fånga in avvikelser om de inte kan rapporteras in på ett enkelt sätt. För en IVA-sköterska som har fullt fokus på sitt arbete att ta hand om patienter är det svårt att också hitta tid att logga in på datorn och rapportera avvikelser. I sådana här situationer kanske det måste vara så enkelt som att vårdpersonalen bara behöver skriva och lämna in en lapp

[17] Direktiv (EU) 2016/1148, ställer krav på informationssäkerhet i offentliga IT-system inom EU.

om vad som har hänt. Informationen kan därefter slussas in i avvikelsesystemet av någon annan på avdelningen, någon som har en dokumenterad kunskap om hur systemet ska användas. För att förbättra rapporteringsfrekvensen till reidarMTP kan det handla om ökad vana av systemet då det är många fält som ska fyllas i.

I en region verkar medicinteknikerna för att inloggningar till tekniska system ändras. I dag behöver vårdpersonalen logga in på datorerna och sina konton med lösenord för att komma åt system och exempelvis journaler. När en annan person behöver komma åt sin användarprofil, är det krångligt att gå ur alla system för en ny användare med alla olika lösenord och system. Under tiden fortlöper verksamheten och information om patienterna på avdelningen behöver finnas tillgänglig. En alternativ lösning där passerkorten kan användas vid tangentborden för inloggning är nu på gång i den regionen. Att en sådan lösning inte redan har implementerats uppges vara en finansieringsfråga som inte har blivit prioriterad.

En annan föreslagen åtgärd är att möjliggöra en automatisk överföring av information från de regionala systemen in till reidarMTP. Region Skåne hade tidigare en sådan lösning där de certifierade rapportörerna hade möjlighet att genom en knapptryckning föra över informationen till reidarMTP. Som påpekats i intervjustudien är det dock framför allt bakgrundsarbetet, utredningen kring en avvikelse, som tar tid. Finns det inte tid för att göra bakgrundsarbetet så blir det heller ingen rapport, oavsett hur rapporteringssystemet är utformat. Att tidsbrist är en trolig orsak till utebliven rapportering omnämns i tidigare avsnitt. En intervjurespondent spekulerar i att den medicintekniska funktionen oftast är en serviceorganisation. Med ett konstant flöde av uppgifter finns det inte tid för strategiskt arbete och uppföljning. Verksamheten utgår från en riskmodell och prioriterar enligt den. Här ser intervjurespondenten att MDR kan bidra till att situationen förändras. Med anledning av MDR instiftas inom regionen ifråga just nu en kommitté eller ett råd, som ska hantera frågor om medicintekniska produkter. Den medicintekniska funktionen kommer att representeras i rådet, liksom andra tekniktunga verksamheter och användare av medicintekniska produkter.

Som beskrivs i avsnitt *4.6 Rapportering av IT-relaterade avvikelser* hanteras och utreds avvikelser som rör medicintekniska produkter av olika funktioner inom en region och rapporteras dessutom i olika system. För att avhjälpa den problematiken påtalas behovet av en regional samordnare av avvikelsehantering för medicinteknik (Ylvén, 2020). Behovet av en avvikelsesamordnare som samordnar den tekniska utredningen vid avvikelser framhålls också i LfMt:s vägledning för avvikelsehantering (LfMt, 2018).

5 Diskussion

De nya EU-förordningarna och efterlevnaden av dem är under uppbyggnad, men det finns en tro på att MDR och IVDR samt de därtill hörande vägledningarna och nationella regelverken kommer att förbättra de tre nyckelegenskaperna *vårdens effektivitet och förväntade resultat*, *patientsäkerhet* samt *data- och systemsäkerhet*.

Ingen av de ovan nämnda tre nyckelegenskaperna ska äventyra någon av de andra två. Detta är en förutsättning för en välfungerande och säker vård och bör beaktas i alla riskhanteringsprocesser som hanterar någon form av informations- och cybersäkerhet. Det kan emellertid uppstå situationer där man måste välja mellan att bryta en certifiering av en produkt för att säkerställa cybersäkerheten och att bibehålla certifieringen för att säkerställa att produkten är patientsäker.

Flera intervjuade i denna studie och i andra studier som vi har gjort på FOI uttrycker att säkerhetstänkandet inte är i paritet med den trend och önskan om uppkoppling och enkla appar som finns i hela samhället, också i vården. Det antyds att det ibland är ledningen som driver på utvecklingen och införandet av ”rolig” teknik, utan att den alltid förstår konsekvenserna av införandet av denna.

5.1 MDR och cybersäkerhet

Utvecklingen av hälso- och sjukvården och den omställning och digitalisering som sker där omfattar förutom samspelet mellan medicinteknik och informationsteknik även andra tekniska system som inte faller under rubriken medicinteknik. Även om de medicintekniska systemen är ”närmast” patienten och därmed uppenbart centrala för patientsäkerheten, får man inte glömma att andra informationssystem såsom journalsystem och fastighetssystem också kan ha effekter på vården, vilket kan ge effekter på patientens hälsa.

Ett samspel krävs därför inte bara mellan medicinteknik och IT, utan med omgivningen såsom vårdpersonalen, organisationen uppåt, leverantörerna (både vid upphandling och avvikelser) och myndigheterna.

På systemnivå, det vill säga marknaden för medicintekniska produkter i Europa, ser aktörerna framför sig en ensning som leder till säkrare produkter. Vägen dit kan dock innehålla svåra situationer när man ska se till att den redan befintliga installerade tekniken hos vårdgivarna erhåller rätt typ av reservdelar.

En annan fråga är hur den splittrade ansvarsbilden inom hälso- och sjukvården, med många regioner, flera ansvariga myndigheter, och andra aktörer kan försvåra tillämpningen av regelverk och att den eftersträvade ensningen av produkter inte uppnås.

Samarbete mellan medicinteknik och IT krävs för att förbättra arbetet med cybersäkerhetsarbetet. Frågan är hur de ska kunna mötas för att öka cybersäkerheten

utan att det påverkar patientsäkerheten. Kunskap och kommunikation behöver fortsätta att utvecklas. Att även journalsystem och annan medicinsk mjukvara har fått en högre riskklassificering i den nya lagstiftningen innebär att tillverkare av medicinska informationssystem nu får ytterligare krav på sig.

De vägledningar som på EU-nivå håller på att tas fram kommer sannolikt göra arbetet tydligare och ge ett stöd i processen, men ännu så länge är det många som inte vet hur det ska gå till.

5.2 Anmälda organ

Två stora utmaningar för certifieringen enligt MDR är bristen på anmälda organ och de befintliga anmälda organens bristande kapacitet att ta sig an nya kunder. För Sveriges del kan konstateras att bristen på anmälda organ gör att Sverige blir sårbart, vilket har blivit tydligt under pandemin. Att bli ett anmält organ är förknippat med stora kostnader, kompetensbehov och krav på en oberoende och opartisk organisation.

Även hos tillverkarna är kostnader och kompetensbehov stora, och om de ökande kostnaderna blir för stora riskerar produkter (och mindre tillverkare) att försvinna från marknaden.[18]

Förutom RISE har inget av de anmälda organ som vi har tillfrågat velat ställa upp i denna studie. Orsakerna till detta kan vi endast spekulera i. Det kan bero på att de haft en stor belastning under tiden studien pågått, eftersom tiden för införandet av MDR sammanfaller med tiden för intervjuerna, men det kan finnas andra orsaker. Oavsett vilken eller vilka orsakerna är kan man fundera över vad det betyder att inget av dessa organ finns representerade i resultatet för studien. Deras åsikter hade varit intressanta att ta del av. Bilden av hur det är för de anmälda organen har vi fått från de intervjuade företagen, myndigheterna och RISE.

5.3 Avvikelsehantering

För att rapporteringen ska fungera är det flera enskilda steg som måste fungera och resurser som krävs: från att vårdpersonalen påtalar en avvikelse, till att medicintekniker och vårdpersonal har tid och resurser att utreda och till att informationen läggs in i reidarMTP. En process som behöver vara enkel och prioriteras högre i verksamheten för att vara effektiv eller ens ske.

[18] Anna Lefevre Skjöldebrand, vd för Swedish MedTech, redogör den 16 december 2021 i MedTech Magazine för en medlemsundersökning som genomförts i början av december. Undersökningen visar att det nya regelverket, MDR, har lett till kraftigt höjda certifieringsavgifter, och hälften av de svarande företagen anger att de har plockat bort produkter ur sitt sortiment.

Eftersom det är frivilligt att rapportera till reidarMTP kommer det sannolikt alltid att finnas utmaningar för rapporteringen. Vilken typ av morötter eller piskor som behövs för att få igång denna rapportering är inte uttalat, men det är tydligt att alla som ska rapportera in vill ha tid och mandat att göra det.

Det förefaller finnas en enighet i att reidarMTP fyller en viktig funktion för dem som arbetar med patientsäkerheten i de medicintekniska produkterna. Dock måste antalet inrapporteringar öka för att databasen ska var till god nytta.

EUDAMED är inte uppe på banan än, men det finns förhoppningar om att den liksom det övriga regelverket kommer att bidra till bättre patientsäkerhet.

5.4 Framtida arbete och framgångsfaktorer

Kompetensbehoven är stora. Bland vårdgivare behövs personal som är kunnig inom såväl medicinsk teknik som cybersäkerhet. Ute hos företagen och de anmälda organen behövs personer som är väl förtrogna med mjukvaror, cybersäkerhet, medicinteknik, patientsäkerhet och certifieringar.

De stora företagen som har arbetat länge med certifiering i många länder menar att en framgångsfaktor i arbetet är att läsa på och att vara ute i god tid. Man bör alltså inte vänta till dess att övergångstiden håller på att slut.

Samarbete mellan medicinteknik och IT är en framgångsfaktor för regionernas arbete med de medicintekniska produkterna, oavsett om det handlar om patientsäkerhet eller cybersäkerhet.

6 Slutsatser

Studiens första mål var att studera hur regelverk och certifiering förhåller sig till patientsäkerhet och cybersäkerhet. Det blir i intervjuerna tydligt att regelverk och certifieringar som är till för patientsäkerheten, har påverkan även på cybersäkerheten. I vissa fall är det svårt att förbättra både patientsäkerhet och cybersäkerhet, exempelvis när uppdateringar av mjukvara kräver att en certifiering bryts. I andra fall verkar de följas åt, så att den nya förordningen på sikt kommer att leda till förbättring av båda. Ett exempel på detta är när en cyberattack riskerar att påverka en medicinteknisk produkt negativt och patientsäkerheten därmed minskar. Cybersäkerheten är i detta exempel viktig för patientsäkerheten.

Det andra målet var att analysera hur de nya EU-förordningarna kan komma att påverka arbetet med medicintekniska produkter och medicintekniska informationssystem. De nya EU-förordningarna och de därpå följande föreskrifterna har lett till att även medicintekniska informationssystem nu räknas som medicintekniska produkter. De medicintekniska informationssystemen har reglerats och klassats högre, vilket syftar till att förbättra patientsäkerheten. Medicintekniska avdelningar i regionerna behöver därmed samarbeta ännu närmre både informationssäkerhets- och IT-säkerhetsavdelningar. Även tillverkare och myndigheter behöver arbeta med både patientsäkerhet och IT-säkerhet.

Det finns ett stort behov av personal med särskild kompetens inom såväl medicinteknik och patientsäkerhet som cybersäkerhet. Helst ska dessa personer även ha kunskap om det nya regelverket och certifieringsprocessen. Resurs- och kompetensbehoven finns hos både tillverkare och anmälda organ. Utan dessa resurser riskerar de anmälda organen att inte räcka till för att alla produkter ska komma ut på marknaden.

Det tredje målet var att följa upp 2020 års studie om avvikelser för att analysera hur medicinteknisk personal arbetar med avvikelsehantering. Medicinteknisk personal behöver öka inrapporteringsgraden till reidarMTP, för att reidarMTP ska fylla den funktion, som är tänkt. reidarMTP är tänkt att vara en källa till kunskap om vilka avvikelser som förekommer och vilka händelser som kan förebyggas när man känner till dem. Att rapportera till reidarMTP kräver tid för rapportören, men tid ges inte i tillräckligt stor utsträckning. Andra uppgifter prioriteras högre.

För att förbättra rapporteringen av cyberrelaterade avvikelser behövs mer samarbete mellan medicinteknisk och IT-teknisk personal. Kunskapen behöver höjas, kommunikationen förbättras, och i vissa fall behöver organisationsstrukturen förändras för att underlätta samarbetet.

7 Referenser

7.1 Intervjuer

Eidenskog, D. (den 14 augusti 2020). Analytiker, FOI. (U. Eckersand, & J. Wahrenberg, Intervjuare)

Holmgren, M. (den 9 oktober 2020). Förvaltningsledare för reidarMTP. (U. Eckersand, Intervjuare)

IVO - intervju. (den 4 maj 2021). (E. Mittermaier & A-S. Stenérus, Intervjuare)

Läkemedelsverket - intervju. (den 24 september 2021). (E. Mittermaier & A-S. Stenérus Dover, Intervjuare)

Region Gävleborg. (den 12 maj 2021). (E. Kock, E. Mittermaier, & J. Wahrenberg, Intervjuare)

Region Jämtland Härjedalen. (den 27 maj 2021). (U. Eckersand, E. Kock, & E. Mittermaier, Intervjuare)

Region Sörmland. (den 26 maj 2021). (E. Mittermaier, & J. Wahrenberg, Intervjuare)

Region Västra Götaland IT. (den 8 juli 2021). (U. Eckersand, & A.-S. Stenérus Dover, Intervjuare)

Region Västra Götaland MT. (den 21 maj 2021). (U. Eckersand, & A.-S. Stenérus Dover, Intervjuare)

RISE - intervju. (den 8 september 2021). (E. Mittermaier, & A-S. Stenérus, Intervjuare)

Ylvén, J. (den 4 november 2020). 1:e Ingenjör, Avdelning Vårdens Digitalisering, Koncernstab Digitalisering, Västra Götalandsregionen. (U. Eckersand, Intervjuare)

Önne, C. (den 3 november 2020). Handläggare IT/OT-säkerhet, MSB. (U. Eckersand, & J. Wahrenberg, Intervjuare)

7.2 Rapporter, vägledningar och myndighetsdokument

Arbetsmiljöverket. (den 27 maj 2020). *CE-märkning*. Hämtat från Arbetsmiljöverket: https://www.av.se/produktion-industri-och-logistik/produktutformning-och-ce-markning/ den 24 november 2020

Banck, M. (den 17 september 2019). *Vårdhandboken*. Hämtat från Ce-märkning: https://www.vardhandboken.se/arbetssatt-och-ansvar/medicintekniska-produkter/markning/ den 06 augusti 2021

Eckersand, U., & Wahrenberg, J. (2020). *NCS3 - Medicintekniska produkter. CE-märkning och certifiering.* Totalförsvarets forskningsinstitut.

Eckersand, U., & Wahrenberg, J. (2021). *NCS3 - Medicintekniska produkter. Avvikelsehantering.* Totalförsvarets forskningsinstitut.

Elsäkerhetsverket. (den 18 december 2017). *EU-försäkran*. Hämtat från https://www.elsakerhetsverket.se/yrkespersoner/tillverkare-aterforsaljare/de-olika-produktkraven/eu-forsakran/ den 8 december 2020

EU. (den 4 november 2020). *CE-märkning*. Hämtat från Europeiska Unionens officiella webbplats: https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_sv.htm den 8 december 2020

EU. (den 19 oktober 2020). *Standarder i Europa*. Hämtat från Europeiska Unionens officiella webbplats: https://europa.eu/youreurope/business/product-requirements/standards/standards-in-europe/index_sv.htm den 3 november 2020

EU-kommissionen. (2021). *Medical Devices - EUDAMED*. Hämtat från Overview: https://ec.europa.eu/health/md_eudamed/overview_en den 10 maj 2021

EU-kommissionen. (november 2021). *Nando (New Approach Notified and Designated Organisations) Information System.* Hämtat från https://ec.europa.eu/growth/tools-databases/nando/

Hedtjärn Swaling, V., & Mossberg Sonnek, K. (2016). *NCS3 - Beroenden till industriella informations- och styrsystem. En förstudie.* . Totalförsvarets forskningsinstitut.

Holm, H., & Westring, E. (2015). *NCS3 - Informations- och styrsystem inom hälso- och sjukvård. En kartläggning av produkter och incidenter.* FOI.

Ingemarsdotter, J., Hedtjärn Swaling, V., & Eidenskog, D. (2020). *Vilse i lasagnen? En upptäcksfärd i den svenska digitaliseringens mångbottnade problemstruktur.* Totalförsvarets forskningsinstitut.

LfMt. (2018). *Vägledning – Avvikelsehantering och hantering av säkerhetsmeddelanden för medicintekniska produkter.* LfMt.

Lindahl, D., Liljedahl, B., & Waleij, A. (2020). *Cyberattacks in the healthcare sector during the first three months of the covid-19 pandemic.* Totalförsvarets forskningsinstitut.

Läkemedelsverket. (2013). *Vägledning för tillverkare av medicintekniska produkter för in vitro-diagnostik.* Vägledning. Hämtat den 29 juni 2020

Läkemedelsverket. (den 19 januari 2021). *Anmälda organ*. Hämtat från Läkemedelsverket: https://www.lakemedelsverket.se/sv/medicinteknik/anmalda-organ#hmainbody1

Myrén, K. (den 12 juni 2020). *Ackreditering eller certifiering?* Hämtat från SWEDAC: https://www.swedac.se/ackreditering-eller-certifiering/ den 2 december 2020

SIS. (juni 2021). *EU och standarder*. Hämtat från Svenska Institutet för Standarder: https://www.sis.se/standarder/vad-ar-en-standard/eu-och-standarder/ den 3 november 2020

Socialstyrelsens termbank. (den 17 december 2020). Hämtat från https://termbank.socialstyrelsen.se/

SOU 2021:19. (den 31 mars 2021). En stärkt försörjningsberedskap för hälso- och sjukvården. Sveriges regering, Socialdepartementet.

7.3 Standarder och regelverk

IVDR. (den 5 april 2017). *Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU*. EU. Hämtat från https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:02017R0746-20170505&from=EN den 16 november 2020

MDR. (den 5 april 2017). *Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices*. EU. Hämtat från https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:02017R0745-20170505&from=EN den 16 november 2020

Patientdatalagen. (2008:355).

Socialstyrelsens föreskrifter om användning av medicintekniska produkter i hälso- och sjukvården (HSLF-FS 2021:52). (u.d.).

Svensk standard, SS-EN 80001-1. (2011). *Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter - Del 1: Roller, ansvar och aktiviteter.* Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/medicinsk-utrustning/allmant/ssen800011/ den 27 november 2020

Svensk standard. SS-ISO 16142-1:2017 . (2017). *Erkända grundläggande principer för säkerhet och prestanda för medicintekniska produkter - Del 1: Allmänna grundläggande principer och ytterligare särskilda principer för medicintekniska produkter som inte är IVD produ.* Hämtat från Svenska Institutet för Standarder: https://www.sis.se/api/document/preview/8025712/ den 30 november 2020

7.4 Nyhetsartiklar

https://www.kalix.se/, tillfällig webbplats för Kalix kommun, besökt 21 december 2021.

MedTech Europe. (den 5 November 2020). *The first module of EUDAMED on Actor registration to be launched in December*. Hämtat från News: https://www.medtecheurope.org/news-and-events/news/the-first-module-of-eudamed-on-actor-registration-to-be-launched-in-december/ den 10 maj 2021

Mårtensson, S. (den 10 maj 2019). *striktare krav för med-tech produkter – är ni redo för nya mdr?* Hämtat från morris law: https://www.morrislaw.se/nyheter/striktare-krav-foer-med-tech-produkter-aer-ni-redo-foer-nya-mdr-368220/ den 30 november 2020

Swedish MedTech. (den 31 Oktober 2019). *EUDAMED lanseras i maj 2022*. Hämtat från

https://www.swedishmedtech.se/nyheter/2019/10/31/eudamed-lanseras-i-maj-2022.aspx den 10 maj 2021

Swedish Medtech. (den 11 maj 2021). Hämtat från Brist på anmälda organ för in-vitro diagnostik: https://www.swedishmedtech.se/nyheter/2021/5/11/brist-pa-anmalda-organ-for-in-vitro-diagnostik.aspx

TÜV SüD. (2021). *Vertrauen in eine nachhaltige och digitale Zukunft aufbauen.* Hämtat från TÜV SüD - über uns: https://www.tuvsud.com/de-de/-/media/de/corporate/pdf/ueber-uns/tuev-sued-imagebroschuere.pdf den 29 november 2021

Vestvik-Lunde, J. (den 31 maj 2018). *DNV GL acquires 100% ownership of Presafe*. Hämtat från DNV - Healthcare: https://www.dnv.com/news/dnv-gl-acquires-100-ownership-of-presafe-122380 den 29 november 2021

7.5 Film

Lindahl, D. (2021). *Rikskonferensen Folk och Försvar*. Hämtat från Folk och försvar: https://www.youtube.com/results?search_query=folk+och+f%C3%B6rsvar+2021

Bilaga 1. Intervjufrågor

Följande intervjufrågor är hämtade från de två memon som skrevs i förstudien som gjordes under 2020 (se Eckersand & Wahrenberg (2020) *NCS3 - Medicintekniska produkter. CE-märkning och certifiering* och Eckersand & Wahrenberg (2021) *NCS3 - Medicintekniska produkter. Avvikelsehantering*). Först presenteras frågorna om CE-märkning och därefter frågorna om avvikelsehantering. Alla frågor har inte ställts till alla intervjuade. Vissa frågor som rör cybersäkerhet, har av sekretesskäl inte kunnat ställas.

CE-märkning

Syftet med intervjuerna är att identifiera vilka konflikter som inom ramen för regelverken kan uppstå mellan att säkerställa patientsäkerhet och cybersäkerhet.

Tillverkare – bakgrundsfrågor

Vilka medicintekniska produkter tillverkar ni? Hur stora volymer? Till vilken marknad? Hur många anställda är ni?

Tillverkare - regelverk

Vilka standarder måste ni uppfylla för att kunna sälja era medicintekniska produkter?

Vilka certifieringar använder ni för era produkter? Vem certifierar er?

Hur arbetar ni med de nya EU-förordningarna? Behöver ni uppfylla MDR eller IVDR eller båda? Vad gör ni med de produkter i ert sortiment som inte klarar förordningskraven?

Berörs era produkter av andra direktiv? Finns det några motsatsförhållanden mellan olika direktiv och förordningar?

Har ni utsett någon sakkunnig för att ni ska kunna efterfölja regelverket?

Hur ser ni på EUDAMED, den europeiska databasen där ni ska registrera era produkter och dit ni ska rapportera eventuella olyckor och tillbud?

Hur fungerar er styrning när det gäller patientsäkerhet? Saknas något?

Hur fungerar er styrning när det gäller cybersäkerhetsfrågor? Saknas något?

Fungerar samarbetet med föreskrifts- och tillsynsmyndigheterna bra?

Tillverkare - patientsäkerhet och cybersäkerhet

Hur arbetar ni med patientsäkerhetsfrågor?

Vilka verktyg har ni för att arbeta med patientsäkerhetsfrågor? Hur utbildas personalen i dessa frågor?

Hur arbetar ni med cybersäkerhetsfrågor?

Hur arbetar ni med säkerhetstester? Gör ni säkerhetsanalyser? Vilka andra verktyg använder ni i cybersäkerhetsarbetet?

Hur hanterar ni uppdateringar av den mjukvara ni bygger in i era produkter? Hur hanterar ni andra mjukvaruuppdateringar som berör era produkter?

Ser ni någon konflikt mellan patientsäkerhet och cybersäkerhet i någon av era produkter eller i den verksamhet som de ska användas? Har ni identifierat några konflikter generellt mellan patientsäkerhet och cybersäkerhet?

Vilka fördelar ser ni med certifiering? Vilka fördelar ser ni med den nya EU-förordningen?

Vad är de största problemen med certifiering, den nya EU-förordningen ur ett patientsäkerhetsperspektiv och ur ett cybersäkerhetsperspektiv?

Saknar ni något i regelverk eller standarder när det gäller cybersäkerhet generellt och mjukvaruuppdatering specifikt?

Vårdgivare

Inför intervjuer med vårdgivare är det viktigt att få en balans mellan representanter för den medicintekniska och den IT-tekniska sidan för att få en så rättvisande bild av hur arbetet med patientsäkerhet, vårdeffektivitet och cybersäkerhet fungerar i vården.

Vårdgivare - bakgrundsfrågor

Vilket är ert verksamhetsområde? Hur många anställda är ni? Hur stort geografiskt område har ni ansvar för?

Vilka grupper av medicintekniska produkter arbetar ni med? Vilka medicintekniska produkter har ni som är digitala på något sätt? Digitala men ej uppkopplade? Uppkopplade mot något internt system? Uppkopplade mot Internet?

Vårdgivare - regelverk

Hur arbetar ni med standarder och certifieringar?

Har ni satt upp några egna krav på patientsäkerhet eller cybersäkerhet i er utrustning (utöver lagstadgade)?

Hur arbetar ni med de nya EU-förordningarna (MDR och IVDR)? Vad gör ni om produkter som ni behöver inte klarar de nya kraven och därmed inte finns tillgängliga?

Hur fungerar er styrning när det gäller patientsäkerhet? Saknas något?

Hur fungerar er styrning när det gäller cybersäkerhetsfrågor? Saknas något?

Fungerar samarbetet med föreskrifts- och tillsynsmyndigheterna bra?

Vårdgivare - patientsäkerhet och cybersäkerhet

Hur arbetar ni med patientsäkerhetsfrågor? Vilka verktyg har ni för att arbeta med patientsäkerhetsfrågor?

Hur arbetar ni med cybersäkerhetsfrågor? Vilka verktyg har ni för att arbeta med cybersäkerhetsfrågor? Hur arbetar ni med säkerhetstester? Gör ni säkerhetsanalyser? Hur skyddar ni era nätverk mot intrång? Hur hanterar ni mjukvaruuppdatering (t.ex. operativsystem eller annan inbyggd mjukvara) i era produkter? Vad gör ni med äldre utrustning som inte har uppdaterats på många år? Vilka har behörighet att ändra i systemen? Hur utbildas personalen?

Vad gör ni för patientsäkerhetsåtgärder när ni får en ny medicinteknisk produkt? Vad gör ni för cybersäkerhetsåtgärder när ni får en ny medicinteknisk produkt?

Är tillverkarnas anvisningar tillräckliga för ert arbete med patientsäkerhet och cybersäkerhet? Händer det att ni ifrågasätter tillverkarens anvisningar?

Ser ni någon konflikt mellan patientsäkerhet och cybersäkerhet i någon av de produkter ni använder eller i er verksamhet? Har ni identifierat några konflikter generellt mellan patientsäkerhet och cybersäkerhet?

Hur kommunicerar ni med den medicintekniska avdelningen/den IT-tekniska avdelningen? (Frågan anpassas efter vilken avdelning intervjupersonen befinner sig på.) Har ni ett fungerande samarbete?

Vilka är de största problemen med certifiering och den nya EU-förordningen ur ett patientsäkerhetsperspektiv och ur ett cybersäkerhetsperspektiv?

Saknar ni något i regelverk eller standarder för att det ska bli tydligare i ert arbete när det gäller cybersäkerhet generellt och mjukvaruuppdatering specifikt?

Vårdgivare - egentillverkning

Tillverkar ni några medicintekniska produkter själva? Om ja, programmerar ni mjukvara själva eller köper ni in färdiga produkter? Om nej, varför inte?

Modifierar ni produkter som ni köpt in? Ändrar ni något då i mjukvaror? Varför eller varför inte?

Går det med dagens regelverk (och morgondagens MDR) att ändra i ett system eller en produkt? Går det att bygga egen utrustning?

Myndigheter

Vilken roll har myndigheten när det gäller medicintekniska produkter? Kan du beskriva vad arbetet innebär? Hur många anställda är ni som arbetar med föreskrifter/tillsyn?

Hur förändras ert arbete av de nya EU-förordningarna?

Vilken roll har ni om det visar sig att någon produkt måste bort från marknaden för att den inte uppfyller det blir för kostsamt att uppfylla kraven i MDR eller IVDR för produkten? Kan ni påverka detta? I så fall, hur?

Ser ni någon problematik som gör att patientsäkerheten får stå tillbaka för cybersäkerheten eller tvärtom? Hur arbetar ni med problematiken kring patientsäkerhet och cybersäkerhet i medicinteknisk utrustning? Saknar ni något i regelverk eller standarder för att det ska bli tydligare vad som gäller?

Vilka åtgärder har ni möjlighet att vidta?

Hur kommunicerar ni med vårdgivare och tillverkare om problematiken? Hur fungerar samarbetet med vårdgivare och tillverkare?

Arbetar ni med någon föreskrift kring detta? (endast för föreskriftsmyndighet)

Arbetar ni med någon vägledning för att hjälpa vårdgivarna eller tillverkarna?

Hur hjälper ni vårdgivare och tillverkare att få kunskaper om förordningar, föreskrifter och standarder?

Upptäcker ni problem vid tillsyn? (endast tillsynsmyndighet)

Avvikelsehantering

Frågorna i denna del handlar om hur avvikelserapportering kan utvecklas och användas för de avvikelser som berör cybersäkerhet och hur medicinteknisk personal i samverkan med IT-personal arbetar med cybersäkerhet. De nya EU-förordningarna berörs också i frågorna. Frågorna riktar sig främst till medicinteknisk och IT-teknisk personal hos vårdgivare samt föreskrifts- och tillsynsmyndigheter.

Vårdgivare – avvikelsehantering

Rapporterar du in avvikelser? Hur länge har du gjort det? I vilken roll rapporterar du?

Hur upplever du att avvikelsehanteringen fungerar hos er?

Följer ni (din avdelning eller enhet) någon särskild rutin eller vägledning för att rapportera avvikelser? [vilken eller vilka?]

Hur rapporterar ni in avvikelser? Hur ofta rapporterar ni in avvikelser? Vem rapporterar in avvikelser hos er? Vart rapporterar ni in avvikelser? [databaser, reidarMTP, myndigheter]

Har ni upplevt några problem vid rapportering av avvikelser till reidarMTP?

Hur skiljer sig er rapportering till reidarMTP från den rapportering ni gör till den regionala databasen? [mängdmässigt och innehållsmässigt] Skiljer sig reidarMTP från er regionala databas? Skulle du ha nytta av en koppling mellan den regionala databasen och reidarMTP?

Vilken nytta har ni av reidarMTP? Abonnerar ni på någon tjänst från reidarMTP? Använder ni de rapporter om avvikelser som finns i databasen? På vilket sätt?

Antalet avvikelser som rapporteras till reidarMTP minskar från redan låga nivåer. Vad tror du att det beror på? Ser ni en liknande minskning i inrapporteringen till den regionala databasen? Vilken typ av avvikelser tror ni döljer sig bland de avvikelser som aldrig har rapporterats in? Hur stort är mörkertalet?

Vad motiverar dig att ta dig tid att rapportera in en avvikelse? Vad hindrar dig? Har du något förslag på vad som skulle kunna öka rapporteringsfrekvensen till reidarMTP?

Om du fick designa ett avvikelserapporteringssystem, hur skulle du göra det? Vilka funktioner eller inmatningsfält saknar du idag? Vilka funktioner eller inmatningsfält är överflödiga?

Vad tycker du är det bästa med reidarMTP? Vad tycker du är det sämsta?

Behövs reidarMTP?

Vårdgivare – cybersäkerhet i medicintekniska produkter

Hur kan datorrelaterade fel (mjukvara eller hårdvara) och cybersäkerhetsrisker, -hot eller -sårbarheter bättre lyftas i avvikelserapporteringen?

Vi hittar endast en rapport om en DDoS-attack och en händelse gällande en zero day-sårbarhet inrapporterad till reidarMTP mellan 2015 och 2020. Varför tror du inte fler cybersäkerhetsrelaterade avvikelser rapporterats in?

Vart skulle du rapportera om ni fick ett cyberrelaterat intrång i någon medicinteknisk utrustning? Rapporterar du avvikelsen på samma sätt om det är en cyberrelaterad avvikelse som om det är en sladd som lossnat av misstag?

På vilket sätt skulle reidarMTP vara användbart för att förebygga ett cyberangrepp? Kan reidarMTP användas för att hantera och åtgärda ett pågående cyberangrepp? Hur kan man använda reidarMTP efter ett cyberangrepp för att på bästa sätt förhindra liknande händelser?

Vilka rutiner har ni för viruskontroller och brandväggar?

Vilka rutiner har ni för säkerhetsuppdateringar?

Vem får installera mjukvara?

Vilka rutiner har ni för säkerhetskopiering? Testar ni återläsning?

Vilka rutiner har ni för behörigheter?

Vilka rutiner har ni för inloggning? Hanterar ni flerfaktorsautentisering?

Vilka rutiner har ni för övervakning och loggning?

Genomför ni säkerhetsanalyser av utrustningen innan den ansluts till ett nätverk?

Hur arbetar ni med nätverkssegmentering?

Vilka aktörer (personalkategorier, föreningar, myndigheter) anser du behöver agera för att förbättra cybersäkerheten i de medicintekniska systemen? Vad önskar du att de gör?

Hur är ert samarbete kring cybersäkerhet med leverantörer och tillverkare av medicintekniska produkter? Tycker ni att de är lyhörda för de krav som ställs på cybersäkerheten?

Hur arbetar ni med cybersäkerhet när ni upphandlar medicintekniska produkter?

Hur arbetar ni med cybersäkerhet när ni upphandlar organisationsgemensamma administrativa system, nätverk, servrar eller mjukvaror?

Hur arbetar ni med patientsäkerhet när ni upphandlar organisationsgemensamma administrativa system, nätverk, servrar eller mjukvaror?

Vårdgivare – samarbete

Hur kan medicinteknisk personal och IT-personal tillsammans arbeta för att öka cybersäkerhet?

Hur är ert samarbete? Talar ni samma språk? Förstår ni varandra? På vilket sätt skiljer sig er syn på cybersäkerhet i de medicintekniska produkterna från deras?

Hur hanterar ni avvikelser?

Hur hanterar ni incidenter?

Är det någon skillnad på hur ni använder begreppen avvikelse och incident?

Vad är hårdvara? Vilken typ av avvikelser bör rapporteras in som orsakade av hårdvarufel?

För att undvika cyberattacker är det inte bara tekniken som är viktig. Handhavandet kan vara minst lika viktigt. Är det något ni diskuterat tidigare eller något ni arbetar med nu? Vilka åtgärder behöver vidtas för att förbättra handhavandet?

Hur kan ni, medicinsk teknik och IT, tillsammans förbättra kunskaper om både patientsäkerhet och cybersäkerhet?

Fråga till IT: Vilken åtgärd kan medicinsk teknik vidta, som du anser är den viktigaste för att förbättra cybersäkerheten i medicintekniska produkter?

Fråga till MT: Vilken åtgärd kan IT vidta, som du anser är den viktigaste för att förbättra cybersäkerheten i medicintekniska produkter?

Myndigheter – avvikelsehantering

Hur tror ni att avvikelserapporteringen i Sverige kommer att påverkas av de förändrade kraven på rapportering till EUDAMED? På kort sikt och på lång sikt?

Hur upplever ni att avvikelserapporteringen fungerar idag? [bra, förbättringspotential]

Hur tar ni hand om de avvikelser som rapporteras till er?

Hur återkopplar ni er analys till vården, tillverkarna och leverantörerna? Vad händer därefter?

Hur ser ni på den nationella databasen reidarMTP? Använder ni den? På vilket sätt?

Antalet avvikelser som rapporteras till reidarMTP minskar. Vad tror du att det beror på? Spelar det någon roll för patientsäkerheten i Sverige? Hur ser det ut i er databas (Läkemedelsverket)?

Hur ser ni på de regionala databaserna? Använder ni dem? På vilket sätt?

Finns det något problem med att det finns databaser på flera olika nivåer (regionalt, nationellt och EU-nivå)?

Påverkar förändringarna av EUDAMED er databas (Läkemedelsverket)? Hur? Tror ni förändringarna i EUDAMED kommer att påverka inrapporteringen till reidarMTP?

Kommer reidarMTP att behövas på sikt? Kan man samordna alla databaser till en?

Myndigheter – cybersäkerhet i medicintekniska produkter

Arbetar ni med några nya föreskrifter eller vägledningar som rör cybersäkerhet i medicintekniska produkter? När beräknas de komma? Vad handlar de om?

Påverkar den nya EU-lagstiftningen hur ni arbetar med föreskrifter eller vägledningar för cybersäkerhet i medicintekniska produkter? Om ja, hur? Om nej, varför inte?

Hur arbetar din myndighet med att implementera MDR och IVDR?

Vilka myndigheter behöver delta i arbetet för att förbättra cybersäkerheten i medicintekniska system? Är arbetet som bedrivs idag tillräckligt? Hur kan myndigheter samarbeta om dessa frågor? Vilka mandat har ni att agera?

Få cyberattacker har rapporterats in i reidarMTP. Hur kan inrapporteringen av cybersäkerhets-relaterade avvikelser förbättras? Generellt men också specifikt i den nationella databasen?

Bilaga 2. Begrepp och förkortningar

Cyberteknik:

Cybersäkerhet (i denna rapport likställt med *IT-säkerhet*) är ett begrepp som i denna rapport omfattar såväl organisatoriska som tekniska åtgärder vilka genomförs för att skydda cybersystem mot obehörig åtkomst och angrepp (Merriam-Webster Online Dictionary, 2021, egen övers.). Åtgärderna skyddar indirekt systemens funktion och den information som systemen hanterar.

DDos-attack, *Distributed Denial of Service attack*, är en attack som sker när illvilliga aktörer aktivt överbelastar ett system. Det är vanligt att synkroniserade attacker genomförs med hjälp av enorma mängder data eller botnät (stor mängd kapade datorer för överbelastningsattacker). Attackerna riktas mot nätverk, system eller specifika IT-tjänster och kan genomföras med relativt enkla medel. Risken att utsättas för en DDoS-attack finns i alla samhällsfunktioner, företag och organisationer som är uppkopplade till nätverk (MSB, 2014) och (U.S. Department of Homeland Security, 2021).

Informationssäkerhet. EU-organet för cybersäkerhet, ENISA, definierar informationssäkerhet som skydd mot hot om stöld, borttagning eller förändring av lagrade eller överförda data i ett cybersystem (ENISA, 2021, egen övers.). Enligt standarden SS-EN 27000 definieras informationssäkerhet som ”bevarande av konfidentialitet, riktighet och tillgänglighet hos information” med tillägget att det även kan ”inkludera egenskaper som autenticitet, ansvarsskyldighet, oavvislighet och tillförlitlighet” (Svensk standard. SS-ISO 16142-1:2017).

IT-säkerhet se *cybersäkerhet.*

NIS-direktivet (EU-direktiv 2016/1148) ställer krav på informationssäkerhet i nätverk och IT-system hos leverantörer av samhällsviktig verksamhet (MSB, 2021).

Zero-day. Zero day-sårbarheter innebär sårbarheter som inte är kända för varken utvecklare, leverantörer eller användare. Olika aktörer utnyttjar sårbarheterna för att få tillgång till system, få administratörsrättigheter eller kunna utföra någon typ av aktivitet i systemet. Flera kända zero day-fall har uppdagats, bland annat i en TCP-IP-stack (mjukvaran i ett kommunikationsprotokoll) som är vanlig i IoT (Internet of Things) och andra produkter tillverkade av etablerade leverantörer såsom HP, Intel och Schneider Electric. Dessa sårbarheter har möjliggjort tillgång till nätverk och enheter på distans och att systemen har kunnat tas över av en angripare. Ett exempel på detta är Stuxnetmasken, som utnyttjade flertalet zero day-sårbarheter i Windows vilka tidigare var okända för både allmänheten och leverantören. Stuxnet orsakade att fysiska komponenter och cyberfysiska system kunde manipuleras (Ablon & Bogart, 2017), (CERT-SE, 2020) och (ENISA - Glossary).

Medicinteknik:

Anmälda organ, Notified Bodies, är oberoende företag och organisationer ”som bistår och övervakar tillverkarnas arbete med att verifiera att produkterna uppfyller EU:s regelverk. Detta sker genom provning, kontroll och certifiering i enlighet med EU:s rättsakter” (SWEDAC - Anmälda och utsedda organ. https://www.swedac.se/tjanster/anmalda-och-utsedda-organ/). I Sverige är det Swedac som bedömer, utser och utövar tillsyn över anmälda organ. Swedac anmäler organen till EU-kommissionen som förtecknar alla anmälda organ i databasen Nando.

EUDAMED, European database on medical devices, är det IT system som används för att övervaka både säkerhet och prestanda i de medicintekniska produkter som regleras av antingen MDR eller IVDR (Medical Device Regulations and EUDAMED 2021).

IVD, In Vitro Diagnostic Medical Devices Directive 98/79/EC, är Europaparlamentets och Rådets direktiv 98/79/EG från den 27 oktober 1998 om medicintekniska produkter för in vitro-diagnostik.

IVDR, In Vitro Diagnostic Regulation, är EU-förordning 2017/746 om medicintekniska produkter för in vitro-diagnostik.

LfMT, Ledningsnätverket för Medicinsk Teknik, är sjukvårdshuvudmännens gemensamma forum för samverkan, erfarenhetsutbyte och utveckling inom det medicintekniska området. Sjukvårdshuvudmännen företräds av medicintekniska chefer eller motsvarande (LfMT. https://lfmt.se/om-lfmt).

MDD, Medical Device Directive är Rådets direktiv 93/42/EEG från den 14 juni 1993 om medicintekniska produkter.

MDR Medical Device Regulation, Regulation (EU) 2017/745 om medicintekniska produkter.

Medicinteknisk produkt definieras enligt artikel 2 i MDR som ett:

> instrument, apparat, anordning, programvara, implantat, reagens, material eller annan artikel som enligt tillverkaren är avsedd att, antingen separat eller i kombination, användas på människor för ett eller flera av följande medicinska ändamål, nämligen
>
> – diagnos, profylax, övervakning, prediktion, prognos, behandling eller lindring av sjukdom,
>
> - diagnos, övervakning, behandling, lindring av eller kompensation för en skada eller funktionsnedsättning,
>
> - undersökning, ersättning eller ändring av anatomin eller av en fysiologisk eller patologisk process eller ett fysiologiskt eller patologiskt tillstånd,

- tillhandahållande av information genom undersökning in vitro av prover från människokroppen, inklusive donationer av organ, blod och vävnad,

och som inte uppnår sin huvudsakliga, avsedda verkan i eller på människokroppen med hjälp av farmakologiska, immunologiska eller metaboliska medel, men som kan understödjas i sin funktion av sådana medel.

Nando, New Approach Notified and Designated Organisations, en databas över anmälda organ i Europa.[19]

reidarMTP, nationell databas för inrapportering av avvikelser i medicinteknisk utrustning.

Referenser till Bilaga 2

Ablon, L., & Bogart, A. (2017). *Zero Days. Thousands of Nights. The Life and Times of Zero-Day Vulnerabilities and Their Exploits.* Hämtat från RAND corporations: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1751/RAND_RR1751.pdf den 10 februari 2021

CERT-SE. (den 17 juni 2020). *Kritiska Zero day sårbarheter i TCP/IP-stack (Ripple20).* Hämtat från https://www.cert.se/2020/06/kritiska-zero-day-sarbarheter-i-treck-bibliotek-for-tcp-ip den 10 februari 2021

ENISA - Glossary. (u.d.). Hämtat från https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/zero-day den 10 februari 2021

ENISA. (2021). *Definition of Cybersecurity - Gaps and overlaps in standardisation*. Hämtat från https://www.enisa.europa.eu/publications/definition-of-cybersecurity den 30 augusti 2021

LfMT. https://lfmt.se/om-lfmt. (u.d.). *Om LfMT.* Hämtat från https://lfmt.se/om-lfmt den 10 februari 2021

Medical Device Regulations and EUDAMED 2021. (u.d.). Hämtat från https://eudamed.com/index.php/2021/01/18/medical-device-regulations-and-eudamed-2021/ den 8 december 2021

Merriam-Webster Online Dictionary. (2021). Hämtat från https://www.merriam-webster.com/dictionary/cybersecurity den 30 augusti 2021

[19] För mer information om Nando, se https://ec.europa.eu/growth/tools-databases/nando/

MSB. (2014). *Att hantera överbelastningsattacker*. (Myndigheten för samhällsskydd och beredskap) Hämtat från https://rib.msb.se/filer/pdf/27385.pdf den 9 februari 2021

MSB. (2021). *NIS-direktivet*. Hämtat från https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ den 7 december 2021

NIS-direktivet, EU-direktiv 2016/1148

SWEDAC - Anmälda och utsedda organ. https://www.swedac.se/tjanster/anmalda-och-utsedda-organ/. (u.d.). Hämtat den 8 december 2021

Svensk standard. SS-ISO 16142-1:2017 . (2017). *Erkända grundläggande principer för säkerhet och prestanda för medicintekniska produkter - Del 1: Allmänna grundläggande principer och ytterligare särskilda principer för medicintekniska produkter som inte är IVD produ.* Hämtat från Svenska Institutet för Standarder: https://www.sis.se/api/document/preview/8025712/ den 30 november 2020

U.S. Department of Homeland Security. (2021). *Distributed Denial of Service Defence,*. Hämtat från https://www.dhs.gov/science-and-technology/ddosd den 9 februari 2021

Bilaga 3. Standarder

Svensk standard. SS-EN ISO 14971:2020. Medicintekniska produkter – Tillämpning av ett system för riskhantering för medicintekniska produkter fastställdes 2020. Denna standard handlar om riskhantering för samtliga medicintekniska produkter, inklusive medicintekniska mjukvaror, och avser risker med bland annat data- och systemsäkerhet (Svensk standard. SS-ISO 16142-1:2017 , 2017). I standarden exemplifieras vad som behöver vara med när man identifierar risker och konsekvenser vid användande av medicintekniska produkter. Standarden berör såväl tillgänglighet, integritet och konfidentialitet för information som funktionalitet i medicinsk diagnostik och övervakning. Några cyberrelaterade osäkerheter som nämns är externt tillgängliga portar, okrypterade data och sårbarheter i mjukvara (Svensk standard · SS-EN ISO 14971:2020, 2020, ss. 3, 39).

Svensk standard. SS-EN 80001-1. Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter - Del 1: Roller, ansvar och aktiviteter är en standard från 2011 som är tänkt att användas för att hantera risker i IT-nätverk där medicintekniska produkter ingår. I processen för att hantera riskerna i det medicintekniska nätverket ingår för vårdgivaren att dokumentera och planera riskhanteringen, identifiera de risker som kan uppkomma, föreslå åtgärder så att oacceptabla risker kan bedömas som acceptabla. Riskhanteringsprocessen omfattar även installation, anslutning, konfiguration, drift och underhåll av det medicintekniska IT-nätverket (Svensk standard, SS-EN 80001-1, 2011).

Svensk standard. SS-ISO 16142-1:2017. Erkända grundläggande principer för säkerhet och prestanda för medicintekniska produkter - Del 1: Allmänna grundläggande principer och ytterligare särskilda principer för medicintekniska produkter som inte är IVD-produkter och guide till val av standarder. Det är en standard som kan användas för alla medicintekniska produkter som inte omfattar in-vitro diagnostik. Standarden gäller delvis också för in-vitro-diagnostik-produkter när det avser de generella principerna för säkerhet och prestanda, men standarden beskriver även ytterligare väsentliga principer för säkerhet och prestanda för medicintekniska produkter som inte är in-vitro-diagnostik-produkter. Standarden identifierar också andra särskilt viktiga standarder som behöver uppmärksammas för att den medicintekniska produkten ska vara säker att använda (Svensk standard. SS-ISO 16142-1:2017 , 2017).

Svensk standard. SS-ISO 16142-2:2018. Erkända grundläggande principer för säkerhet och prestanda för medicintekniska produkter - Del 2: Allmänna grundläggande principer och ytterligare särskilda principer för alla IVD-produkter och guide till val av standarder. Den fastställdes 2018 och liknar SS-ISO 16142-1 i det att den beskriver de generella principerna för säkerhet. Standarden utökar SS-ISO 16142-1 genom att beskriva ytterligare väsentliga principer för IVD-produkter (Svensk standard, SS-ISO 16142-2:2018, 2018).

IEC standard. IEC 62304:2006. Medical device software - Software life cycle processes är en internationell standard som definierar krav på mjukvarors livscykler och livscykelprocesser (IEC STANDARD · IEC 62304:2006, 2006). IEC 62304 tar upp risker som kan förknippas med de negativa effekter som kan uppstå vid interaktionen mellan mjukvara och dess omgivning (Svensk standard. SS-ISO 16142-1:2017 , s. 28). Standarden beskriver att medicintekniska produkter, som själva är mjukvara eller som har inbyggd eller integrerad mjukvara, ska vara utformade för att ha en säker och pålitlig prestanda och att lämpliga medel ska användas för att se till att risker minimeras eller elimineras (Svensk standard. SS-ISO 16142-1:2017 , 2017, ss. 30-31).

IEC standard. IEC 60601-1:2005. Medical electrical equipment - Part 1: General requirements for basic safety and essential performance är en annan internationell standard som rör säkerhetskrav och väsentlig prestanda hos elektriska medicintekniska produkter (IEC STANDARD · IEC 60601-1:2005, 2005). IEC 60601-1 tar precis som IEC 62304 upp risker som kan förknippas med de negativa effekter som uppstår vid interaktionen mellan mjukvaran och dess omgivning, att mjukvaran ska utformas så att den är säker och pålitlig samt att risker ska minimeras eller elimineras med lämpliga metoder (Svensk standard. SS-ISO 16142-1:2017 , ss. 28-31).

IEC standard. IEC TR 80002-3:2014. Medical device software - Part 3: Process reference model of medical device software life cycle processes är en teknisk rapport som beskriver medicintekniska mjukvarors livscykelprocesser. Rapporten bygger på IEC 62304 (se ovan), ISO/IEC 12207:2008 och ISO/IEC 24774:2010. De båda sistnämnda standarderna rör livscykelprocessen och förvaltningen av mjukvara generellt medan den första standarden specifikt rör mjukvara i medicinsk teknik (IEC STANDARD · IEC TR 80002-3:2014, 2014).

Referenser till Bilaga 3

IEC STANDARD · IEC 60601-1:2005. (2005). *Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*. Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/medicinsk-utrustning/iec6060112005/ den 1 december 2020

IEC STANDARD · IEC 62304:2006. (2006). *Medical device software - Software life cycle processes*. Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/medicinsk-utrustning/iec-623042006-eee96df2/ den 1 december 2020

IEC STANDARD · IEC TR 80002-3:2014. (2014). *Medical device software - Part 3: Process reference model of medical device software life cycle processes (IEC 62304)*. Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/medicinsk-utrustning/allmant/iectr8000232014/ den 1 december 2020

Svensk standard · SS-EN ISO 14971:2020. (2020). *Medicintekniska produkter - Tillämpning av ett system för riskhantering för medicintekniska produkter (ISO 14971:2019)*. Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/kvalitetsledningssystem-inom-halso-och-sjukvard/medicintekniska-kvalitetssystem/ss-en-iso-1497120202/ den 30 november 2020

Svensk standard, SS-EN 80001-1. (2011). *Riskhantering tillämpad på IT-nätverk som innehåller eller är kopplade till medicintekniska produkter - Del 1: Roller, ansvar och aktiviteter.* Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/medicinsk-utrustning/allmant/ssen800011/ den 27 november 2020

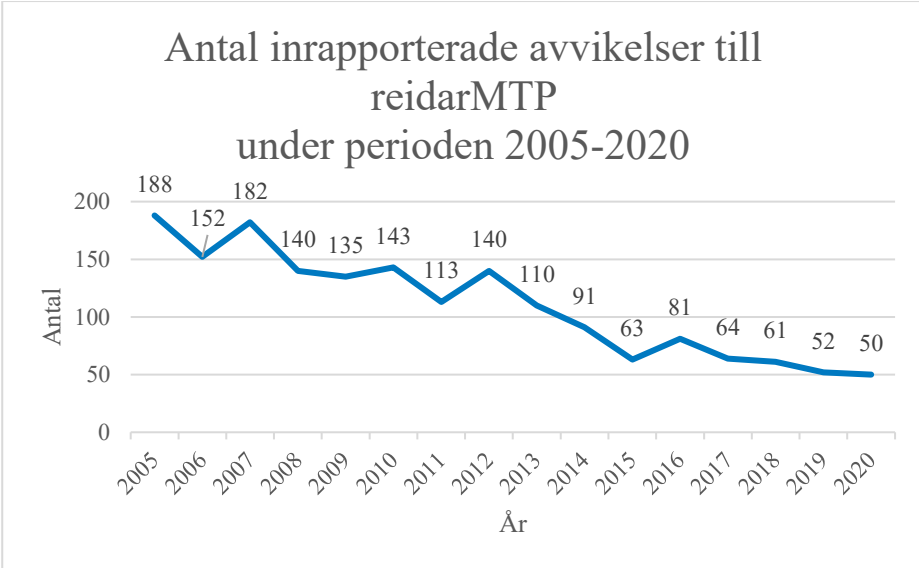
Svensk standard, SS-ISO 16142-2:2018. (2018). *Erkända grundläggande principer för säkerhet och prestanda för medicintekniska produkter - Del 2: Allmänna grundläggande principer och ytterligare särskilda principer för alla IVD produkter och guide till val av standarder (ISO 16142-2:2017, IDT)*. Hämtat från Svenska Institutet för Standarder: https://www.sis.se/produkter/halso-och-sjukvard/medicinsk-utrustning/ss-iso-16142-22018/ den 30 november 2020

Svensk standard. SS-ISO 16142-1:2017 . (2017). *Erkända grundläggande principer för säkerhet och prestanda för medicintekniska produkter - Del 1: Allmänna grundläggande principer och ytterligare särskilda principer för medicintekniska produkter som inte är IVD produ.* Hämtat från Svenska Institutet för Standarder: https://www.sis.se/api/document/preview/8025712/ den 30 november 2020

Bilaga 4. Avvikelsestatistik

I denna bilaga redovisas med hjälp av diagram antalet avvikelser som har rapporterats in till reidarMTP under åren 2005-2020, vilka orsakerna till avvikelserna är och hur fördelningen mellan olika typer av avvikelser har varit.[20]

Under åren 2005 och 2006 rapporterades 340 avvikelser in till reidarMTP, vilket kan jämföras med 371 för de sex åren mellan 2015 och 2020. (Se figur 1.)

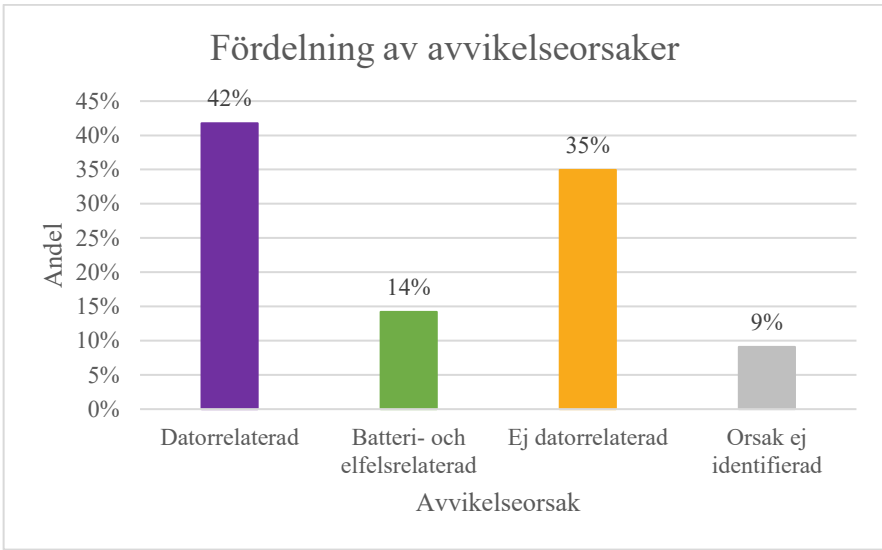


Figur 1. Antal inrapporterade avvikelser till reidarMTP under perioden 2005-2020.

Dessa siffror kan jämföras med inrapporteringen till regionala databaser. På Sahlgrenska sjukhuset rapporteras ungefär 1000 avvikelser in varje år i den regionala databasen (Ylvén, 2020). En uppskattning som gjorts från de avvikelserna är att ungefär mellan 10 och 20 % av dessa rör medicintekniska produkter och skulle behöva rapporteras in nationellt till reidarMTP (Ylvén, 2020). Det skulle motsvara mellan 100 och 200 årliga avvikelser bara från Sahlgrenska Universitetssjukhuset, vilket alltså från bara ett sjukhus är långt många fler än vad som rapporteras in årligen till reidarMTP.

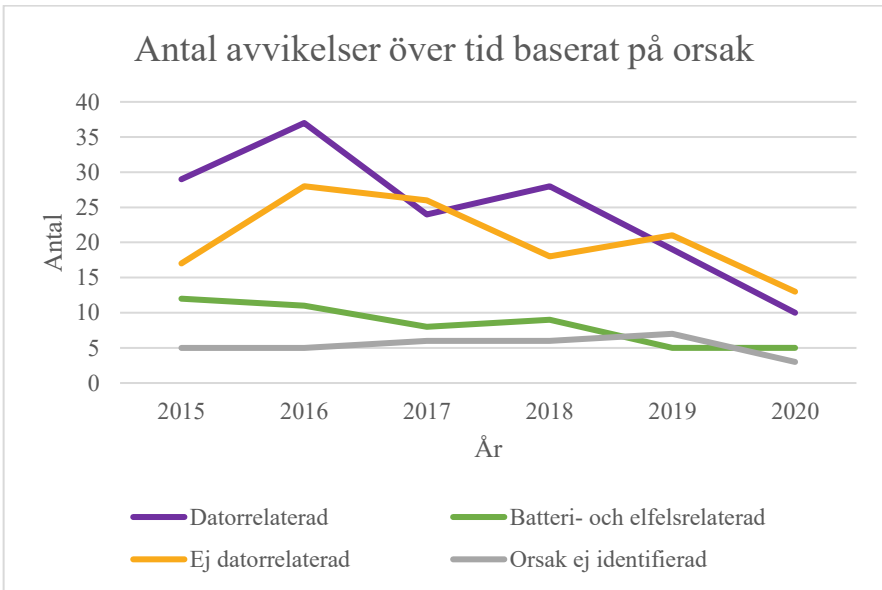
Avvikelserna kategoriserades i datorrelaterade, batteri- och elfelsrelaterade samt ej datorrelaterade fel. (Se figur 2.)

[20] För mer information om statistiken och hur den har tagits fram hänvisas till Eckersand & Wahrenberg, *NCS3 - Medicintekniska produkter. Avvikelsehantering.* (2021)



Figur 2. Fördelning mellan olika orsaker till avvikelser under perioden 1 januari 2015-30 september 2020.

Antalet avvikelser, som har rapporterats in till reidarMTP, har under en längre tid minskat som figur 1 visar. Inrapporteringen av de datorrelaterade avvikelserna har minskat under de senaste fem åren. (Se figur 3.)



Figur 3. Antal avvikelser mellan 1 januari 2015 och 30 september 2020 baserat på bakomliggande orsak.

Det finns enbart två avvikelseärenden som är tydligt relaterade till cybersäkerhet. Det första ärendet är *Kritiska zero day-sårbarheter i TCP/IP-stack (Ripple20)* (Ärendenummer Reidar-002459) som inträffade den 17 juni 2020 och registrerades den 26 juni 2020. Denna avvikelse är inte inrapporterad för att något tillbud har inträffat i vården, utan är till för att upplysa användare av TCP-IP-stackar om att det finns en inbyggd sårbarhet och att ett antal medicintekniska produkter kan vara påverkade. Den som har rapporterat in hänvisar till säkerhetsmeddelanden från respektive tillverkare och leverantör för vidare information.

Det andra ärendet relaterat till cybersäkerhet, är den enda avvikelsen som rapporterats in som orsakad av en attack. Rubriken på avvikelsen är *Långt kommunikationsavbrott* (Ärendenummer Reidar-002159) registrerades den 13 juni 2016, men inträffade redan den 23 februari 2016. Avvikelserapporten beskriver att data inte har kunnat överföras från ”Checkupväskor i länet till den centrala databasen” mellan 23 februari och slutet av mars. Orsaksutredningen visar att den bakomliggande orsaken är en DDos-attack och därpå följande nedstängning av servern. Därefter kunde driften av väskorna[21] inte startas.

Referenser till Bilaga 4

Ylvén, J. (den 4 november 2020). 1:e Ingenjör, Avdelning Vårdens Digitalisering, Koncernstab Digitalisering. (U. Eckersand, Intervjuare) Västra Götalandsregionen.

[21] Väskor som används vid vårdbesök i hemmen. Innehåller bland annat hjärtstartare, snabbtester för sänka, blodvärde och sockernivåer, termometer, blodtrycks- och blodgasmätare. (Hemsjukvård; http://www.checkup.se/?t=u&s=12461&hs=12448 besökt senast 8 februari 2021.)

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se