Datum: 2024-04-24

Institutionen för ekonomi och IT

Avdelningen för informatik

IT-säkerhet, i händerna på en läkare

- En kvalitativ studie om läkares IT-säkerhetsmedvetenhet samt attityder och erfarenheter kring personliga enheter inom sjukvården.

Författare:

Joachim Åhlström

Magnus Uskali

Kandidatuppsats, 15 HP

Examensarbete i informatik

Vårterminen 2024

Handledare: Helena Vallo Hult

Examinator: Lars Svensson

IT-security, in the hands of a doctor

Joachim Åhlström

Magnus Uskali

Abstract

As cyberattacks against healthcare increase, it becomes important for healthcare caregivers to maintain robust IT security to protect patient data. Previous research has shown that gaps in employees' awareness of IT security, insufficient guidelines and policies, and outdated digital tools often lead to healthcare personnel using risky workarounds. One such workaround is the use of personal devices in daily work. This qualitative study explores doctors' awareness of IT security as well as their attitudes and experiences regarding the use of personal devices within healthcare. Through a literature review and individual interviews, data has been collected and analyzed to highlight key aspects of IT security and Bring Your Own Device (BYOD) in healthcare settings. The results reveal deficiencies in IT security training, the need for reliable digital tools, and the prevalence of workarounds in daily work. The conclusions emphasize the importance of continuous IT security training, adapted digital technology, and clear guidelines for the use of personal devices. Suggestions for further research include conducting a quantitative study on doctors' awareness of IT security nationwide in Sweden and investigations into how hospital administrations manage guidelines regarding personal devices. The study contributes to a deeper understanding of IT security and BYOD in healthcare and highlights important areas for further improvements and ongoing research.

Keywords

IT security, IT security awareness, BYOD, Workarounds, Healthcare, Doctor, Healthcare Staff, Patient Data.

IT-säkerhet, i händerna på en läkare

Joachim Åhlström

Magnus Uskali

Sammanfattning

I takt med att cyberangrepp mot sjukvården ökar, blir det allt viktigare för vårdgivare att upprätthålla en robust IT-säkerhet för att skydda känslig patientdata. Tidigare forskning har visat att brister i anställdas IT-säkerhetsmedvetenhet, otillräckliga riktlinjer och policys samt föråldrade digitala verktyg ofta leder till att sjukvårdspersonal använder sig av riskfyllda workarounds. En sådan workaround är användningen av personliga enheter i det dagliga arbetet. Denna kvalitativa studie utforskar läkares IT-säkerhetsmedvetenhet samt deras attityder och erfarenheter kring användningen av personliga enheter inom sjukvården. Genom en strukturerad litteraturöversikt och individuella intervjuer har data samlats in och analyserats för att belysa viktiga aspekter av IT-säkerhet och Bring Your Own Device (BYOD) i vårdsammanhang. Resultaten pekar på brister i IT-säkerhetsutbildning, behovet av pålitliga digitala verktyg och förekomsten av workarounds i det dagliga arbetet. Slutsatserna betonar vikten av kontinuerlig IT-säkerhetsutbildning, anpassad digital teknik och tydliga riktlinjer för användning av personliga enheter. Förslag till fortsatt forskning inkluderar en kvantitativ studie om läkares IT-säkerhetsmedvetenhet i hela Sverige samt undersökningar om hur sjukhusledningar hanterar riktlinjer kring personliga enheter. Studien bidrar till en fördjupad förståelse av IT-säkerhet och BYOD inom sjukvården och lyfter fram viktiga områden för vidare förbättringar och fortsatt forskning.

Nyckelord

IT-säkerhet, IT-säkerhetsmedvetenhet, BYOD, Workarounds, Sjukvård, Läkare, Sjukvårdspersonal, Patientdata

Förord

Inledningsvis vill vi tacka vår fantastiska handledare Helena Vallo Hult som har hjälpt och stöttat oss under hela arbetets gång samt hjälpt oss med möten och kontakt med respondenter. Vi vill även rikta ett stort tack till alla respondenter som har lagt ned sin tid och deltagit i studien, utan er hade det inte varit möjligt att genomföra vår kandidatuppsats. Slutligen vill vi även tacka de opponenter som har hjälpt oss förbättra vår studie.

Trevlig läsning!

Ordlista

AI-genererad - Information eller innehåll som skapas eller framställs med hjälp av artificiell intelligens.

Bring Your Own Device (BYOD) - Är en praxis där anställda använder sina personliga enheter, såsom smartphones, bärbara datorer och surfplattor, för arbetsrelaterade uppgifter och ansluter dem till företagets nätverk och system.

Cyberangrepp - Är attacker mot datorsystem eller nätverk som syftar till att stjäla information, sabotera system eller på annat sätt orsaka skada.

IT-säkerhet - Handlar om att skydda datorer, nätverk och information från obehörig åtkomst, skadlig programvara och andra hot.

IT-säkerhetsmedvetenhet - Är en individs kunskap eller kännedom om de hot som finns mot IT-säkerhet samt om möjliga säkerhetsåtgärder för att hantera dessa hot.

Kryptering - Är processen att omvandla information till ett oläsbart format med hjälp av en algoritm, vilket gör det svårt att läsa informationen utan rätt åtkomstnyckel.

Patientdata - Är information som rör en individs hälsa och vård, såsom medicinsk historik, diagnoser, behandlingar och personliga uppgifter.

Personliga enheter - I studien avser personliga enheter läkarnas egna mobiltelefoner, surfplattor eller datorer.

Policys - Är regler eller riktlinjer som fastställs av en organisation för att styra beteende, hantering av information, och beslut som tas inom företaget.

Ransomware - Är en typ av skadlig programvara som låser dina filer och kräver pengar för att släppa samt ge tillbaka tillgång till dem.

Workarounds - Alternativa lösningar som används för att kringgå ett problem i befintliga arbetsrutiner.

Förkortningar

Bring Your Own Device (BYOD), Informationsteknik (IT), europeiska byrån för nät- och informationssäkerhet (ENISA), International Business Machines Corporation (IBM).

Innehållsförteckning

1. Inledning

I takt med den ökade digitaliseringen och användningen av digitala verktyg inom sjukvården har IT-säkerhet blivit ett växande bekymmer för vårdgivare (Nifakos m.fl., 2021). Genom att digitalisera vården strävar man efter att förbättra kvaliteten på sjukvården både för vårdpersonal och patienter. Med tillgång till digitala system och enheter inom vården kan man erbjuda högkvalitativ vård mer effektivt (Alkhaledi & Hawamdeh, 2023; Nifakos m.fl., 2021). Eftersom den tekniska utvecklingen växer snabbt så hänger inte IT-säkerheten med i utvecklingen, och det är därför av stor vikt för verksamheter att sprida medvetenhet om IT-säkerhet och vilka åtgärder som bör tas för att skydda känslig data (MSB, 2024).

Trots att digitaliseringen har många fördelar kan det också uppstå nya risker och sårbarheter som kan äventyra sekretessen, integriteten och tillgängligheten av känslig hälsoinformation. Hoten mot digitala journalsystem och patientdata ökar och en stor utmaning är hanteringen av patientdata då det finns brister i medvetenheten och kunskapen om IT-säkerhet bland vårdpersonal (Alkhaledi & Hawamdeh, 2023; Javaid m.fl., 2023). Cyberangrepp mot hälso- och sjukvårdssektorn blir alltmer vanligt då patientdata är ett attraktivt mål som värderas högt. En vanlig metod som kriminella aktörer använder sig av är att kryptera data och sedan utkräva en lösensumma för att återskapa den data som är krypterad. Angripare räknar med att lösensumman blir betald då patientdata är väldig känslig samt att människors liv och hälsa kan stå på spel (MSB, 2024).

Wani m.fl. (2022) påpekar att det har blivit alltmer vanligt att vårdgivare tillåter sin personal att använda sina personliga enheter i det dagliga sjukvårdsarbetet. Konceptet kallas Bring Your Own Device (BYOD) och har blivit ett stort problem för IT-säkerheten inom sjukvården. Med sina personliga enheter kan vårdpersonal dela okrypterad patientdata mellan varandra vilket medför en stor säkerhetsrisk då telefoner lätt kan tappas bort, bli stulna eller utsättas för cyberangrepp (Ranganathan, 2016; Soni, Kukreja & Sharma, 2020). Detta utnyttjar många angripare och riktar sig in på personliga enheter för att komma åt organisationers känsliga data, vilket ökar verksamhetens sårbarhet mot attacker då anställda inte alltid är medvetna om riskerna kopplade till deras användning av sina egna telefoner (Soni, Kukreja & Sharma, 2020).

1.1 Bakgrund

Digitala enheter såsom datorer, smartphones och surfplattor är ett snabbväxande fenomen och arbete med digitala verktyg blir alltmer vanligt i dagens samhälle. I takt med att organisationer och verksamheter över hela världen genomgår en digital förändring så börjar de tydligt uppleva fördelarna med digitaliseringen. Men även om det finns fördelar med digitaliseringen så medför det också stora risker, speciellt riskerna för cyberangrepp (Nifakos m.fl., 2021). Cyberangrepp är ett ständigt pågående hot och det försämrade säkerhetsläget i världen har gjort att risken för cyberangrepp har ökat. Både främmande makt och andra kriminella aktörer använder sig av cyberangrepp för att inhämta information eller genomföra sabotage. Eftersom detta är ett ständigt pågående hot så är det av stor vikt att organisationer ser till att skydda sig mot dessa angrepp (Säkerhetspolisen, 2022).

För att kunna tackla dessa pågående hot inom IT-säkerhet behöver anställda utbildning om ämnet. Många branscher erbjuder idag någon form av IT-säkerhetsutbildning för sina anställda, men de har svårt att motivera och engagera medarbetarna till att vilja lära sig om de risker och hot som finns (Chowdhury, Katsikas & Gkioulos, 2022). Europeiska unionens byrå för nät- och informationssäkerhet (ENISA) betonar vikten av att öka nivån av kunskap och färdigheter om IT-säkerhet då det är en mycket viktig faktor för att bygga upp samhällets motståndskraft mot cyberangrepp (ENISA, 2017). Forskning har visat att utbildning kan vara effektivt för att stärka lämpligt beteende och användningen av teknologi för att skydda verksamheters känsliga data (Hepp m.fl., 2018). Många nuvarande IT-säkerhetsutbildningar har inte utvecklats i samma takt som de teknologiska framstegen, vilket är särskilt tydligt inom hälso- och sjukvården. En dåligt utformad IT-säkerhetsutbildning kan innebära att vårdpersonal får en bristande kunskap om vilka risker som finns kring hantering av patientdata bland vårdpersonal (Bellwood m.fl., 2011; Hepp m.fl., 2018).

En form av cyberangrepp som har blivit vanligt förekommande mot sjukvården är social manipulation, som riktar in sig på att utnyttja vårdpersonalen (Nifakos m.fl., 2021). Således är det viktigt att få ökad förståelse för de risker och hot som är kopplade till IT-säkerhet för att kunna bedriva en skyddad och säkrare vårdmiljö. Därmed måste sjukvården säkerställa att medvetenheten om IT-säkerhet bland vårdpersonal är hög samt att det bedrivs utbildning om IT-säkerhet (Nifakos m.fl., 2021). En säkrare vårdmiljö är synnerligen relevant och viktig då sjukvården är väldigt utsatt. Idag används digitala hälsosystem som kan ge fördelar både för patientvård och för att effektivisera sjukvårdens arbete (Hepp m.fl., 2018). Men information

om patienters hälsa lagrade i digitala journalsystem utsätter även en risk för patienters integritet och säkerhet (Hepp m.fl., 2018). För läkare är patienters fysiska hälsa och välbefinnande mycket viktig och det bör finnas riktlinjer samt regler om hur man hanterar information om patienter på ett säkert sätt. Dessa riktlinjer är viktiga att följa för att skydda patientdata (Nilsson, Törner & Pousette, 2018). Men ibland kan det uppstå konflikter mellan patienters fysiska hälsa och dessa riktlinjer. Vid dessa tillfällen måste läkarna agera genom att ta egna beslut och då går patientens fysiska hälsa före eventuella säkerhetsöverträdelser (Nilsson, Törner & Pousette, 2018).

1.2 Problemformulering

Anställda utgör vanligtvis måltavlor för cyberangrepp genom social manipulation, ofta via e-post med skadliga webblänkar, vilket understryker behovet av medvetenhet och utbildning kring sådana manipulativa försök (Green & Dozier, 2023). Många av de cyberincidenter som inträffar är på grund av bristande kunskap eller IT-utbildning hos de anställda. 74 procent av alla cyberbrott som begås beror på den mänskliga faktorn och bland de mest allvarliga incidenterna är det en femtedel som uppstår på grund av att människor har agerat felaktigt eller att de blivit utsatta för social manipulation (Mikuletič m.fl., 2024). Det är ett stort risktagande av organisationer när policys saknas eller har brister samtidigt som medvetenheten om säkerhetsfrågor bland medarbetarna är låg. Generellt finns ett stort behov av att höja medvetenheten om IT-säkerhet hos alla medarbetare för att få en säkrare hantering av känslig information (MSB, 2020).

Etiska frågor är ett problem inom IT-säkerhet, speciellt inom sjukvården. Den ökande användningen av digitala system och enheter inom vården för att övervaka patienters hälsotillstånd har effektiviserat vården men det väcker också en oro kring hur patienters sekretess och integritet hanteras och skyddas (Pollini m.fl., 2022). Sjukvårdspersonal tenderar att använda sig av sina personliga enheter inom sitt arbete och det är ett koncept som heter Bring Your Own Device (BYOD). Fördelarna med BYOD är att man snabbt kan dela testresultat, rådgöra med kollegor eller svara på larm och på så sätt hjälpa sina patienter mer effektivt (Ranganathan, 2016; Pollini m.fl., 2022). Det förekommer även kritiska IT-säkerhetsöverträdelser då sjukvårdspersonal använder verksamhetskonton med sina personliga telefoner för att ladda ner, lagra eller dela känsliga bilagor mellan varandra. Många vårdanställda brister i kunskap och gör felet att förlita sig på säkerheten i dessa personliga telefoner. Detta utsätter sjukvården för en stor IT-säkerhetsrisk då många telefoner som

används inom sjukvården inte använder sig av kryptering (Ranganathan, 2016; Pollini m.fl., 2022). Att det delas okrypterad patientdata mellan sjukvårdspersonal är oroande och angripare kan utnyttja denna sårbarhet för identitetsstöld eller för att tjäna pengar genom utpressning (Ranganathan, 2016).

Wani m.fl. (2022) menar att det förekommer workarounds inom sjukvården, vilket innebär att anställda hittar alternativa lösningar för att kringgå problem i befintliga arbetsrutiner. En sådan alternativ lösning sker till exempel när läkare använder sina personliga enheter för medicinsk fotografering och delar bilder med sina kollegor via applikationer likt WhatsApp (Wani m.fl., 2022). Även om det finns avsedda kameror på sjukhus för detta ändamål är det opraktiskt att använda dem eftersom det kan ta lång tid att hitta en kamera och ladda upp bilderna till ett system, jämfört med att det bara tar några sekunder om man använder sin personliga enhet (Nerminathan m.fl., 2017). Användningen av BYOD är en stor utmaning för sjukvården då man har begränsad kontroll över hur sjukvårdspersonal använder sina personliga enheter. För att hantera dessa risker krävs policys och riktlinjer för BYOD, men trots detta använder mindre än hälften av alla sjukhus sådana säkerhetsåtgärder. Detta ökar sårbarheten för sjukvården och patientdata utsetts för en stor risk vilket tidigare har lett till flertalet dataintrång inom sjukvården (Wani m.fl., 2022).

Sammanfattningsvis pekar tidigare forskning på att det saknas IT-säkerhetsmedvetenhet inom vården, därför finns ett behov till ökad kunskap bland vårdpersonal för att kunna hantera de utmaningar och IT-säkerhetsrisker som finns. Att utforma strategier och riktlinjer samt erbjuda kontinuerlig IT-säkerhetsutbildning är ett effektivt sätt att bemöta dessa risker och bidrar till en säkrare vårdmiljö för vårdpersonal och patienter. Det finns även ett behov av att täcka en forskningslucka och bidra med mer kunskap om, och förståelse för IT-säkerhetsmedvetenhet, samt attityder och erfarenheter kring personliga enheter inom sjukvården.

1.3 Syfte och frågeställning

Syftet med denna studie är att utforska hur användningen av personliga enheter används bland läkare inom sjukvården. Genom att analysera deras attityder och erfarenheter kring användningen av BYOD-enheter som egna telefoner, bärbara datorer och surfplattor, avser vi få en djupare förståelse för hur dessa enheter integreras i sjukvårdens arbetsflöde och vilken påverkan det får på sjukvårdens IT-säkerhet.

Vilket leder till våra frågeställningar som lyder:

- Hur medvetna är läkare om IT-säkerhet inom sjukvården?
- Hur är läkares attityder och erfarenheter kring Bring Your Own Device inom sjukvården?

1.4 Avgränsningar

Studiens omfattning kommer att avgränsas till sjukhus i en specifik region i Sverige och till läkares attityder och erfarenheter av Bring Your Own Device (BYOD) inom sjukvården, mer specifikt mobiltelefoner, datorer och surfplattor. Utvalda läkare används som nyckelpersoner i studien eftersom de använder sig av personliga enheter på sjukhuset sedan tidigare. Detta gör att läkarna får en central roll i undersökningen av hur IT-säkerhetsmedvetenhet påverkar användningen av BYOD-enheter. Valet av att rikta in sig på BYOD beror på att det är oklart hur läkares attityder och användning av personliga enheter påverkar IT-säkerheten inom sjukvården. Det finns brist på tidigare forskning kring detta vilket motiverar denna inriktning (Wani m.fl., 2022).

2. Teori och tidigare forskning

I följande kapitel presenteras tidigare forskning och teoretiskt ramverk kopplat till studiens syfte. Då studiens syfte är att utforska läkares IT-säkerhetmedvetenhet inom sjukvården samt deras attityder och erfarenheter av personliga enheter kommer detta avsnitt fokusera på tidigare forskning kopplat till dessa områden. Vi kommer också belysa fenomenet med workarounds, då det är vanligt förekommande inom sjukvården.

2.1.1 IT-säkerhet

IT-säkerhet är ett väletablerat område som främst handlar om att skydda datorsystem mot stöld, skada, störningar och olaglig åtkomst till känslig information (Deepa m.fl., 2024). Enligt Wani, Mendoza och Gray (2020) innebär även IT-säkerhet att skydda verksamheters informationsresurser såsom sekretess, integritet och tillgänglighet. Inom sjukvården innebär detta att man måste säkerställa skyddet av kritisk hälsoinformation, till exempel patientdata. Detta kan uppnås genom att tillämpa viktiga säkerhetsåtgärder såsom policys, processer och olika teknologier (Wani, Mendoza & Gray, 2020).

Pfleeger (2015) definierar ett hot som en potentiell händelse som kan resultera i skada, medan en sårbarhet är en brist eller svaghet som kan utnyttjas för att skapa skada. Dessa två faktorer är ofta kopplade till varandra, då ett hot kan realiseras genom att utnyttja en sårbarhet, vilket i sin tur kan resultera i skada. Pfleeger (2015) menar även att det finns tre huvuddelar av ett datorsystem som är särskilt mottagliga för attacker: hårdvara, mjukvara och data. Dessa komponenter, samt kommunikationen mellan dem, är sårbara och kan lätt bli måltavlor för angrepp. Därav är det viktigt att saker skyddas av sekretess, ett exempel på det är medicinska journaler. Definitionen av sekretess är rak, endast auktoriserade personer eller system bör få tillgång till känslig data (Pfleeger, 2015).

Vidare ser Javaid m.fl. (2023) att angripare använder ransomwareattacker för att kryptera och hålla filer som gisslan, vilket leder till att sjukvården inte får tillgång till medicinska journaler eller utrustning. För sjukhus är dessa angrepp ett stort hot mot sjukvården eftersom förlust av patientdata kan äventyra patienters liv (Javaid m.fl., 2023). Det har tidigare förekommit angrepp mot sjukvården, ett exempel är WannaCry-attacken 2017 där tusentals vårdmöten och operationer fick ställas in. Ett annat exempel är ett angrepp mot Singapores SingHealth 2018 där 1,5 miljoner patienters patientdata läckte ut (O'brien, Ghafur & Durkin, 2021). Dessa

angrepp är exempel på hur allvarliga konsekvenserna kan bli av angrepp mot hälso- och sjukvården.

Bristande IT-säkerhet är ett hot som växer, de senaste cyberangreppen mot sjukvården runt om i världen har påvisat vilka risker det finns (O'Brien, Ghafur & Durkin, 2021). Enligt en rapport av IBM och Ponemon har frekvensen av dataintrång mot sjukvården ökat sedan 2010 och den hör nu till de branscher som är en av de största måltavlorna för cyberangrepp globalt (Argaw m.fl., 2020). För att bedriva nödvändig och effektiv patientvård samt meningsfull forskning, behöver man pålitliga system som delar medicinska data inom sjukvården (Argaw m.fl., 2020). Med den globala ökningen av digitala patientjournaler har ett behov uppstått av att ge sjukvårdpersonal lämplig IT-säkerhetsutbildning så att det kan lära sig om denna teknik innan den måste användas i verklig miljö (Bellwood m.fl., 2011). O'Brien, Ghafur & Durkin (2021) menar på att medvetenheten utgör en stor utmaning för säkerheten inom hälsosektorn.

2.1.2 IT-säkerhetsmedvetenhet

Kopplingen mellan IT-säkerhet och patientsäkerhet kan naivt ses som något abstrakt eftersom påverkan av cyberangrepp inte omedelbart ger skada eller dödlighet för patienter (O'Brien, Ghafur & Durkin, 2021). För att förhindra cyberangrepp utvecklas säkerhetsteknologier, policys och regler. Många användare följer inte reglerna eller misslyckas med att praktisera förväntat beteende. Även om de flesta system är tekniskt säkra möjliggörs en stor del av cyberincidenter av mänskliga fel (Chang & Coppel, 2020). Att förstå de mänskliga faktorerna till IT-säkerhet är en av de viktigaste delarna för att ändra människors beteende och deras medvetenhet för säkert arbete (Flores m.fl., 2023). En aspekt som kan ses som positiv är att medvetenheten är högre hos anställda och många är mer medvetna om säkerhetsrisker idag än tidigare (Flores m.fl., 2023). Dock krävs det endast en individ som inte gör rätt för att öppna möjligheter för angripare.

Eftersom de anställdas attityder kring IT-säkerhet är starkt kopplad till utbildning är det avgörande för organisationer att genomföra kontinuerliga utbildningar för att öka IT-säkerhetsmedvetenheten (Kang, Kang & Monsen, 2023). Forskning antyder att lämplig utbildning relaterad till IT-säkerhet är viktig för att förbättra sjukvårdspersonalens kunskap för att säkerställa att de upprätthåller patientsekretess och integritet (Kang, Kang & Monsen, 2023). Dock finns det oftast brister i utbildningsmaterialet eftersom den inte är relaterad till de anställdas roller vilket försämrar deras IT-säkerhetsmedvetenhet (Hepp m.fl., 2018; Wani m.fl, 2022). Därav är det av stor betydelse att vårdgivare har tillgång till utbildningar med innehåll

som fokuserar på integritet och säkerhet som är direkt kopplade till deras specifika yrkesroller. Vårdpersonalens attityder till IT-säkerhet skiljer sig beroende på tidigare utbildning i ämnet. Organisationer bör tillhandahålla olika lättillgängliga utbildningsprogram för att förbättra deras medvetenhet. Därför är det en viktig del att främja en positiv IT-säkerhetskultur för att förbättra attityder, vilket i slutändan kommer att främja de anställdas beteenden (Kang, Kang & Monsen, 2023).

2.2 Bring Your Own Device

Bring Your Own Device (BYOD) är ett koncept där anställda använder sina personliga enheter i sitt dagliga arbete, oftast med egna mobiltelefoner, bärbara datorer eller surfplattor (Wani m.fl., 2022). Enligt Wani m.fl. (2022) är BYOD vanligt förekommande inom alla branscher men sjukvården är en av de ledande branscherna där sjukvårdspersonal tillåts använda sina personliga enheter i stor utsträckning. Det finns stora fördelar med BYOD inom sjukvården, bland annat att sjukvårdspersonal kan förbättra sin effektivitet genom användningen av sin personliga enhet då den ofta finns tillgänglig. Man kan även hjälpa patienter på distans genom digitala vårdmöten vilket minskar den fysiska belastningen på sjukhuset samt att sjukvården kan minska sina kostnader ifall vårdpersonal använder sina egna enheter, vilket innebär att man inte behöver upphandla om nya moderna arbetstelefoner till de anställda (Wani m.fl., 2022). Studier visar att ungefär 90 procent av de anställda inom sjukvården använder sina personliga enheter för att utföra arbetsrelaterade uppgifter (Nerminathan m.fl., 2017; Wani, Mendoza & Gray, 2020). Detta sparar mycket tid för vårdpersonalen då man lättare kan få åtkomst till patientjournaler, testresultat, läkemedelsinformation samt kommunicera med sina kollegor på ett effektivare sätt (Wani, Mendoza & Gray, 2020). Å andra sidan är BYOD en stor utmaning för sjukvården när det gäller IT-säkerhet då sjukvården är den bransch som utsätts för nästan hälften av alla dataintrång världen över (Wani m.fl., 2022). BYOD är en stor orsak till dessa dataintrång då personliga enheter utsätter sjukvården för stora risker då sjukvården inte har någon kontroll över vilken typ av enhet som används eller hur dem används (Wani m.fl., 2022). Enligt Nerminathan m.fl (2017) tar läkare självständiga beslut gällande användningen av sina personliga enheter för att öka effektiviteten i sitt arbete, speciellt vid medicinsk fotografering där det ofta är svårt att bedöma balansen mellan de fördelar och risker som finns.

Allt fler läkare förlitar sig på sina personliga enheter för att hantera patientdata vilket ökar risken för att känslig information hamnar i fel händer (Wani m.fl., 2022). I en stor

undersökning såg man att nästan hälften av alla läkare delar patientdata i form av bilder mellan varandra via SMS eller WhatsApp samt att nästintill alla läkare använder liknande applikationer för att diskutera patientfall (Wani, Mendoza & Gray, 2020). Enligt O'Brien, Ghafur och Durkin (2021) är användningen av personliga enheter en stor utmaning för sjukvården. För att säkerställa att vårdpersonalen hanterar sina personliga enheter på ett säkert sätt krävs det policys och riktlinjer för BYOD. Trots de stora riskerna och hoten mot dessa personliga enheter, använder sig mindre än hälften av alla sjukhus BYOD-policys och riktlinjer (Wani m.fl., 2022). Dessa BYOD-policys ses ha en avgörande roll för att vägleda vårdpersonalens användning av sina personliga enheter för att på ett etiskt och acceptabelt sätt kunna hantera patientdata. Detta bör vara högsta prioritet för sjukvården för att undvika allvarliga dataintrång (Nerminathan m.fl., 2017; Wani m.fl., 2022).

2.3 Workarounds

Definition av workarounds enligt Alter (2014) är en arbetslösning som är en måldriven anpassning, improvisation eller en annan förändring av ett befintligt arbetssystem. Workarounds är ofta drivna av mål, för att kringgå eller minimera påverkan av hinder, praxis, ledningars förväntan eller strukturella begräsningar som upplevs som hinder för arbetssystemet. Det kan även vara för att uppnå önskad nivå av effektivitet eller andra organisations- samt personliga mål (Alter, 2014). En workaround kan även beskrivas som en avvikelse från den avsatta arbetsprocessen som används för att övervinna ett hinder (Patterson, 2018).

IT-säkerhets insatser inom sjukvården stöter dagligen på alltmer motstånd och undanflykter från verksamheten såväl som anställda som endast försöker utföra sitt arbete trots ofta besvärliga och irrationella dataskyddsregler (Koppel m.fl., 2015). Det kan finnas flera anledningar till att använda sig av olika typer av workarounds i sitt arbete. Ett tydligt exempel som finns inom sjukvården är konflikten mellan en patients hälsa och att följa arbetsrutiner (Skyvell Nilsson, Törner & Pousette, 2018). Enligt Skyvell Nilsson, Törner och Pousette (2018) värdesätter vårdpersonal patientens hälsa mer än att följa alla säkerhetsrutiner.

Pollini (2021) menar att verksamheter ofta använder sig av riktlinjer och policys för att guida de anställda till en säker hantering gällande IT-säkerheten. Dock tenderar anställda att använda sig av workarounds när system eller olika digitala verktyg inte är tillräckligt användarvänliga. Detta leder till att sjukvårdspersonal använder sig av sina personliga enheter

på ett riskfyllt sätt för att dela patientdata mellan varandra, men samtidigt kan detta tillvägagångsätt förbättra effektiviteten av patientens vård (Pollini, 2021).

När kliniker ställs inför krav på komplexa säkerhetsåtgärder, som att behöva hantera långa lösenord eller logga in på nytt efter inaktivitet tenderar de att söka lösningar som minimerar tidsförlusten (Wani, Mendoza & Gray, 2020). Detta kan innebära att de använder enkla eller lösenord som är lätta att minnas, delar lösenord med kollegor eller till och med använder kommunikationsapplikationer som inte är säkra, till exempel WhatsApp för att kommunicera. Dessa åtgärder utgör en potentiell risk för sjukvårdens IT-säkerhet (Wani, Mendoza & Gray, 2020). För att tackla dessa utmaningar kan sjukhus erbjuda andra applikationer såsom säkra meddelandefunktioner och fotograferingsverktyg, eller enklare inloggningsmetoder för att få tillgång till sjukhusets applikationer. Genom att tillhandahålla sådana säkra och effektiva alternativ kan man underlätta för kliniker att följa säkerhetsrutiner samtidigt som man bibehåller produktiviteten och effektiviteten i deras dagliga arbete (Wani, Mendoza & Gray, 2020).

3. Metod

I detta avsnitt presenteras de val och metoder som användes vid utförandet av litteratursökning. Även metoder för intervjuer, urval, intervjuguide samt en dataanalys på det insamlade materialet kommer redovisas. Vidare så kommer även de etiska principerna för studien att presenteras.

3.1 Litteratursökning

I studien har vetenskapliga artiklar hämtats från databaserna Business Source Ultimate och Academic Search Premier, tillhandahållna av Högskolan Väst. Syftet med denna litteraturgranskning var att komplettera och fördjupa förståelsen kring ämnet för studien. Ämnet som undersöktes fokuserade på läkares IT-säkerhetsmedvetenhet och attityder samt erfarenheter av personliga enheter inom sjukvården.

För att samla in relevant information genomfördes en strukturerad litteratursökning via de tidigare angivna databaserna. Ämnesord användes för att vägleda sökningen och säkerställa att den inhämtade litteraturen var kopplad till studiens syfte. Dessa ämnesord reviderades och förfinades kontinuerligt under litteratursökningens gång för att säkerställa relevans. Exempel på relevanta ämnesord presenteras i tabell 1 nedan.

Aware*	Employee*	Cybersecurity	Healthcare
Informed	Staff	Cyber security	Hospital
	Doctor*	IT security	Medical
	Worker*	IT-security	

Tabell 1 – Strukturerad litteratursökning

Vid litteratursökningen i Business Source Ultimate och Academic Search Premier användes en kombination av sökord med hjälp av OR logik. Ett exempel på hur sökningen utfördes visas nedan:

1. Aware* OR Informed
2. Employee* OR Staff OR Doctor* OR Worker*
3. Cybersecurity OR Cyber security OR IT security OR IT-security
4. Healthcare OR Hospital OR Medical

Efter att dessa enskilda sökningar utförts, genomfördes en mer specifik sökning med AND logik för att göra en sökning med alla sökorden. Det genomfördes även en filtrering som

inkluderade val av engelska som språk, att artiklarna var vetenskapligt granskade samt att årtalen var mellan 2014–2024. Resultatet av sökningen generade 121 träffar som sedan granskades.

För att öka antalet relevanta artiklar genomfördes en kedjesökning, där referenslistor från relevanta artiklar granskades för att se om de passade studiens syfte. För att säkerställa relevansen hos de valda artiklarna granskades abstrakt och nyckelord. Endast de artiklar som ansågs vara relevanta efter denna initiala granskning lästes mer ingående och inkluderades sedan i den samlade litteraturöversikten.

3.2 Intervju

Den typen av intervju som valdes för studien är individuella intervjuer. Enligt Denscombe (2018) finns det fördelar med individuella intervjuer och det är att forskare kan samla in data direkt från intervjupersonens uppfattningar och synpunkter. Dessutom är intervjuerna lätta att arrangera vilket är en viktig aspekt då denna studie utförs under en kortare tid (Denscombe, 2018). Syftet var att fånga respondenternas åsikter, uppfattningar, känslor och erfarenheter på ett djupgående sätt vilket bidrog till en bättre förståelse för ämnet.

Strukturen som valdes för intervjuerna var semi-strukturerade intervjuer. Det innebär att vi som intervjuare använder en intervjuguide med ämnen och frågor som ska diskuteras (Denscombe, 2018). Denna intervjuguide kan ses i bilaga 1. Detta gav oss möjligheten att vara flexibla och ställa följdfrågor vilket gav respondenterna en möjlighet att utveckla sina svar för att ge en mer rik beskrivning av deras erfarenheter (Denscombe, 2018).

Intervjuerna skedde digitalt genom programvaran Microsoft Teams då dessa läkare befann sig på olika kliniker och platser samt att de hade ett tidspressat schema. Fördelen med digitala intervjuer är att det sparar tid både för respondenter och forskare samt gör det möjligt att genomföra intervjuer med personer på olika geografiska platser (Denscombe, 2018). En liten nackdel var att tekniken strulade med uppkopplingen ett par gånger vilket ledde till kommunikationsproblem.

3.2.1 Urval

Studien utfördes på sjukhus i en specifik region i Sverige där digitala verktyg och personliga enheter används i det dagliga arbetet, vilket görs av samtliga respondenter. Sexton läkare från olika kliniker i Sverige blev inbjudna att medverka i studien. Sju personer har valt att delta frivilligt i studien. Enligt Denscombe (2018) finns det två vägar att gå gällande urval.

Representativt urval som förknippas med kvantitativa data eller explorativt urval som förknippas med kvalitativa data (Denscombe, 2018). För denna studie är explorativt urval det valda tillvägagångsättet då vi valde att göra en kvalitativ studie. Vidare nämner Denscombe (2018) att det finns ytterligare två tillvägagångsätt att använda när man gör ett urval, sannolikhetsurval där man slumpmässigt gör ett urval ur undersökningspopulationen och icke-sannolikhetsurval som innebär att forskare har rätt att bestämma i urvalsprocessen. I denna studie användes ett subjektivt urval då vi handplockade deltagarna, efter rekommendation, med hänsyn till deras relevans, erfarenhet och kunskap kopplat till våra två forskningsfrågor (Denscombe, 2018).

Här nedan i tabell 2 visas respondenternas arbetsroll och hur lång tid intervjun varade:

	Arbetsroll	Längd på intervju
R1	Överläkare	30 min
R2	ST-läkare	45 min
R3	ST-läkare	30 min
R4	ST-läkare	35 min
R5	ST-läkare	25 min
R6	ST-läkare	25 min
R7	ST-läkare	25 min

Tabell 2 – Urval av respondenter

3.2.2 Intervjuguide

En intervjuguide skapades och vi undersökte liknande studiers intervjuguide för att få en bild om hur strukturen kan se ut. Vi valde att genomföra semi-strukturerade intervjuer som metod, vilket innebar att ordningen på frågorna kunde variera. Inledningsvis formulerade vi frågorna fritt utifrån studiens övergripande frågeställning. Trots att många frågor skapades, användes inte alla i den slutgiltiga intervjuguiden, då vi efter en granskning insåg att flera av dessa frågor var slutna och inte skulle ge de nyanserade svar vi sökte. Även frågor som var lika varandra och skulle generera liknande svar togs bort. Tidigare bakgrundsfrågor som gjorde det möjligt att koppla personen till dess svar uteslöts på samma sätt. Efter en handledning justerades intervjuguiden med bättre, mer öppna frågor samt att vi lade till olika teman i intervjuguiden så uppdelningen av frågorna blev bättre.

Under intervjuerna uppmuntrades respondenterna att utveckla sina svar och ge detaljerade förklaringar, vilket Denscombe (2018) betonar som är viktigt i det semi-strukturerade tillvägagångsättet. För att ge respondenterna utrymme att kunna svara relativt fritt var det viktigt att skapa en flexibel intervjuguide som kunde fortsatt vara relevant för studiens syfte.

Nedan, i tabell 3, visas olika teman och några exempelfrågor från intervjuguiden.

Teman	Frågor	Beskrivning
Personliga enheter	• Använder du några personliga enheter, såsom egna telefoner eller datorer för arbetsrelaterade uppgifter?	Denna fråga är till för att generera svar angående respondenternas användning och erfarenhet av sina personliga enheter i arbetet. Detta kan även väcka lite tankar kring medvetenheten kring säkerhet hos respondenterna.
IT-säkerhets-medvetenhet	• Har du fått någon utbildning inom IT-säkerhet i sjukvården?	Denna fråga är till för att se om det bedrivs någon IT-säkerhetsutbildning inom sjukvården samt hur medvetna respondenterna är om IT-säkerhet generellt.
Workarounds	• Kan du ge exempel på situationer där workarounds har använts för att kringgå IT-säkerhetsåtgärder inom sjukvården?	Denna fråga är utformad för att ta undersöka om det förekommer workarounds inom sjukvården som kan underminera IT-säkerheten.

Tabell 3 – Utvalda frågor från intervjuguiden

3.2.3 Genomförande av intervju

Respondenterna kontaktades först via e-post och sedan via telefon vid uteblivet svar. I inbjudningsmejlet presenterade vi oss själva och förklarade syftet med studien. Detta inbjudningsmejl återfinns i bilaga 2 längst ned i dokumentet. Intervjuerna utfördes digitalt via Microsoft Teams, detta tillvägagångsätt användes främst för att lättare kunna utföra intervjuerna då många läkare hade ett pressat tidschema samt jobbade oregelbundna tider. Alla

respondenter hade tidigare använt sig av applikationen och kände sig bekväma med den. Det var även lätt att spela in intervjun och transkribera via Microsoft Teams. Båda författarna turades om att föra intervjun och ställa frågor medan den som inte ledde intervjun antecknade och såg till att transkriberingen fungerade. En pilotintervju genomfördes för säkerställa att intervjuguiden var relevant och korrekt utformad, samtidigt som vi ville få en uppfattning om hur lång tid som behövdes för att genomföra intervjuerna. Vi testade även att all teknik som ljud, bild, inspelning och transkribering fungerade under detta tillfälle. Resultatet av pilotintervjun var så positivt att den inkluderades i studiens analys och resultat. Därefter genomförde vi resterande sex intervjuer med våra respondenter, snittlängden för dessa var ungefär 35 minuter.

Nedan i figur 1 visas ett exempel på den AI-genererade transkriberingen från Teams:

0:6:22.170 --> 0:6:24.460

Respondent 2

Så att ja, jag ser nog flera risker.

0:6:27.700 --> 0:6:32.220

Intervjuare 2

Har personalen fått tillåtelse att använda er av egna telefoner?

0:6:33.420 --> 0:6:39.110

Respondent 2

Ja, det skulle jag säga. Den här appen. Till exempel har vi blivit ombedd och ladda ner då de som använder den.

Figur 1 – AI-genererad transkribering

3.3 Tematisk analys

För att göra en dataanalys på vårt insamlade material från intervjuerna använde vi oss av tematisk analys, vilket är en bra metod att använda sig av i en kvalitativ studie för att analysera och identifiera de mönster och teman som finns i det insamlade materialet (Braun & Clarke, 2006). En tematisk analys passade perfekt för vår forskningsansats då det är en lämplig metod om man vill utforska attityder och erfarenheter kopplat till IT-säkerhet (Green & Dozier, 2023).

Enligt Braun och Clarke (2006) finns det två huvudsakliga tillvägagångsätt för att identifiera teman, antingen genom deduktiv eller induktiv metod. Dock påpekar forskarna att man kan använda en kombination av metoderna eftersom det inte finns några fasta regler för det. Detta kallas för abduktiv metod och för denna studie tillämpade vi det abduktiva tillvägagångsättet för att identifiera de teman som ses nedan i Tabell 4. Först använde vi oss av en deduktiv ansats för att identifiera teorier och tidigare forskning relaterad till IT-säkerhetsmedvetenhet, Bring Your Own Device och Workarounds. Detta gav oss en bra struktur som underlättade analysen av det insamlade materialet. Dessa teman fungerade som vägledning när vi kodade det insamlade materialet för att hitta mönster och kategorier som var relevanta till den tidigare forskningen och våra frågeställningar. Sedan tillämpade vi en induktiv ansats vilket ledde till upptäckten av Digitala verktyg, Utbildning samt Policys och riktlinjer som två nya och intressanta teman som framkom genom de individuella intervjuerna.

Vi började med att gå igenom transkriberingen av intervjuerna och jämförde dem med ljudinspelningarna för att korrigera de felformuleringar som fanns i den automatiserade transkriberingen. Sedan läste vi igenom transkriberingen för att få en första förståelse av det insamlade materialet och för att identifiera tidiga mönster (Braun & Clarke, 2006). Därefter genomförde vi en öppen kodning där vi använde färgkodning för att identifiera olika teman. Till sist markerade vi fraser eller ord med den färg som motsvarade ett visst tema. På detta sätt strukturerade vi det insamlade materialet och kunde identifiera de mest centrala insikterna av läkares IT-säkerhetsmedvetenhet och deras attityder och erfarenheter av personliga enheter inom sjukvården.

Utbildning	
Digitala verktyg	
Workarounds	
Personliga enheter	
IT-säkerhetsmedvetenhet	
Policys och riktlinjer	

Tabell 4 - Färgkodning

3.4 Forskningsetik

Denscombe (2018) betonar fyra huvudprinciper inom forskning som utgör grunden för etik och dessa principer är: skydda deltagarnas intressen, garantera att deltagandet är frivilligt, undvika falska förespeglingar samt följa den nationella lagstiftningen.

I studien skyddar vi deltagarnas intressen genom att behandla deras information och svar med strikt sekretess. För att säkerställa detta anonymiserar vi respondenternas arbetsplatser och identiteter samt att citeringar från respondenter inte avslöjar deras identitet (Denscombe, 2018). All data som samlas in kommer hanteras på ett säkert och korrekt sätt för att förhindra obehörig åtkomst samt att materialet inte kommer lagras längre än nödvändigt.

I studien informerar vi om samtycke samt garanterar respondenterna att deltagandet i studien är frivilligt. Vi hade en första kontakt med läkare som var intresserade av att delta i studien och via vår handledare fick vi deras kontaktuppgifter. Redan vid inbjudan till studien bad vi deltagarna att bekräfta sitt samtycke till att delta i studien. Under studiens gång låter vi respondenterna ha full kontroll över sin medverkan och de kan när som helst välja att avbryta eller avstå en intervju utan att behöva ge en förklaring (Denscombe, 2018). I samband med de digitala individuella intervjuerna ber vi om samtycke kring ljud- och videoinspelning.

I studien undviker vi falska förespeglingar då vi klart och tydligt har kommunicerat studiens syfte och vilken information vi har önskat samla in både skriftligt och muntligt, detta för att skapa en öppenhet mellan oss och våra respondenter (Denscombe, 2018). Dessutom har vi informerat respondenterna om hur det inspelade materialet kommer att hanteras. Samtliga respondenter har även erbjudits möjligheten att ta del av det färdiga arbetet.

I studien följer vi nationell lagstiftning genom att hantera personuppgifter med högsta sekretess. Vi kommer att följa kraven för Dataskyddsförordningen (GDPR) vilket innebär att respondenternas uppgifter kommer att anonymiseras och eventuell information gällande etniska bakgrund, politiska åsikter, hälsa, sexuell läggning tas bort om det skulle dyka upp. Studenter råder även under särskilda undantag vilket innebär att vi som författare inte behöver söka etiskt tillstånd för denna studie (Högskolan Väst, 2024).

4. Resultat

I detta avsnitt sammanfattas den insamlade data från de tidigare nämnda intervjuerna. Data har kategoriserats enligt de sex identifierade teman som presenterats i Tematisk analys avsnittet. Vi har delat in dessa teman i rubriker och underrubriker.

4.1 Brist på IT-säkerhetsutbildning hos läkare

Det framkommer under flera av intervjuerna att respondenterna inte fått någon typ av utbildning kring IT-säkerhet, R1 menar på att det kan ha skett ett utbildningstillfälle när man var nyanställd och R4 är osäker på om det ens har förekommit en IT-säkerhetsutbildning.

> ”*Jag har haft min anställning i över 10 år. Det är möjligt att man har fått någon utbildning när man är nyanställd kring IT-säkerhet, men det kan jag inte minnas att jag fått och det är ingenting jag fått uppdaterat*.” (R1)

> *“Spontant skulle jag säga att jag inte fått någon IT-säkerhetsutbildning, men jag har säkert läst något dokument, men det är ingenting som jag kan komma ihåg.”* (R4)

Några respondenter betonar dock att de haft en utbildning om sekretesslagstiftningen och hur man ska hantera och använda patientjournaler. Respondenterna förväntas kunna hela biten om IT-säkerhet trots att man inte fått en utbildning om dess risker och hot. Den digitala utvecklingen har under de senaste tio åren gjort att läkare arbetar annorlunda idag och R6 menar att det behövs IT-säkerhetsutbildningar för att öka medvetenheten: *“[...] det förväntas att man ska kunna den biten, men sen har det ju hänt jättemycket inom IT jämfört med 10 år sedan, då använde man ju inte alls mejl, teams eller sin egna telefon på det här sättet så det skulle behöva fräschas upp egentligen.”*

Däremot menar R5 att det har förekommit en IT-säkerhetsutbildning nyligen i år som hjälpte till att öka IT-säkerhetsmedvetenheten: *[...] jag har nyligen gått en grundläggande IT-säkerhetsutbildning på sjukhuset, vilket har ökat min medvetenhet och minskat risken för påverkan utifrån [...].*”

Respondenterna upplever att IT-säkerhetsutbildningar är något som måste ske kontinuerligt med tanke på alla IT-hot och angrepp som sker mot sjukvården. Olika angripare och aktörer utvecklar hela tiden sina angreppsmetoder och därför behövs det månatliga uppdateringar för att kunna agera på ett säkert sätt. R3 menar att: “*[...] vi skulle behöva få en månatlig uppdatering för att kunna vara medvetna och agera på ett medvetet sätt.”*

4.1.1 Ingen anpassad IT-säkerhetsutbildning

Samtliga respondenter berättade att de inte får någon anpassad IT-säkerhetsutbildning som passar deras roll eller arbetsmiljö. Just nu får alla anställda samma typ av utbildning och den tar inte hänsyn till vilken bakgrund eller förmåga man har som läkare. Respondenterna beskriver att det behövs en mer anpassad utbildning för att fånga intresset hos läkare kring IT-säkerhet. Samtidigt är det viktigt att utbildningsmaterialet inte är för tråkigt eller irrelevant, något som R2 tar upp: "*[...] för närvarande verkar det som att samma IT-säkerhetsutbildning distribueras till hela personalgruppen utan hänsyn till deras bakgrund eller förmåga att ta till sig information. Det finns en potential för förbättring genom att anpassa materialet för olika målgrupper. Det är viktigt att undvika att materialet blir för tråkigt eller irrelevant för att säkerställa att läkare engagerar sig och tar till sig viktig information."*

Vidare förklarar R4 att det behövs en IT-säkerhetsutbildning som är bunden till vad det finns för risker som läkare och vilka situationer som kan uppstå i den dagliga verksamheten. Detta får medhåll från R5 som tycker att den nuvarande IT-säkerhetsutbildningen är för generell och att den inte är sjukvårdsanpassad, istället tar utbildningen upp risker som kan ske på vanliga kontor.

> *"Jag upplevde att IT-säkerhetsutbildningen var väldigt generell.*
> *Den innehöll väldigt basala saker men också tips som bygger på att man har ett visst arbetssätt som vi inte har på sjukhuset."* (R5)

4.1.2 IT-säkerhetsutbildningen blir bortprioriterad

Flera av Respondenterna menar på att läkare är ofta under tidspress och behöver kontinuerligt genomgå olika utbildningar för att utvecklas inom sitt yrke. Detta resulterar att utbildning kring IT-säkerhet ofta nedprioriteras framför andra utbildningar.

> " […] *det förekommer en betydande mängd utbildningar, främst tillgängliga på intranätet, inom läkargruppen. Tyvärr tenderar många av dessa utbildningar att hamna på obestämd tidpunkt och prioriteras inte alltid tillräckligt högt*." (R2)

> "*Vi har en mängd digitala utbildningar som behöver genomföras, men det är svårt att hitta tid för dem, inklusive IT-säkerhetsutbildningar. Det är en utmaning att balansera dessa utbildningar med våra andra åtaganden.*" (R3)

Då det redan finns många obligatoriska utbildningar kring andra arbetsuppgifter som läkare har blir det svårt att hinna med allt, Detta förklarar R4; *"Vi får redan väldigt mycket utbildning inom olika administrativa uppgifter. Och det går inte att ta till sig allting."*

4.2 Saknad av pålitliga digitala verktyg

Samtliga respondenter betonar att bristen på pålitliga digitala verktyg leder till frustration över nuvarande arbetsrutiner. De påpekar även att många arbetsprocesser är ohållbara vilket hindrar dem att arbeta på ett effektivt och säkert sätt. Nyare digitala verktyg och system är något som önskas för att respondenterna ska kunna hjälpa patienter mer effektivt men även skydda deras patientuppgifter på ett bättre sätt. Ett exempel på ett system med brister är det nuvarande journalsystemet då det finns funktioner som ingen vet hur dem ska användas, R2 förklarar: *"[...] det tas inte fram information om programmen i journalsystemet. Det är ett dåligt journalsystem där det finns massa funktioner som inte används för att ingen vet hur de ska användas."* Just nu är man inne i en övergång till ett nytt journalsystem som heter Millenium men det drar ut på tiden och därför använder man mer sårbara lösningar i väntan på något bättre. R6 berättar: *"Vi håller på att byta journalsystem […] det skulle vara implementerat för två år sen men det har fortfarande inte kommit igång och då använder man en mindre optimal och mer sårbar lösning i väntan på övergången."*

4.2.1 Föråldrade enheter och processer

Det framkommer att samtliga respondenter tycker att det används föråldrade enheter och system inom sjukvården. Många av dessa enheter och system är svårarbetade och möter inte längre sjukvårdens behov, något som R7 tar upp: *"[...] vi har för gamla system, de är svårarbetade och möter inte våra behov."* Ett exempel som samtliga respondenter tar upp är arbetsprocessen kring medicinsk fotografering där läkarna ska använda en äldre systemkamera för att lägga till bilder i patientjournalen. Detta arbetssätt är dock alldeles för omodernt och krångligt vilket R3 förklarar nedan:

> *"Jag skulle gissa att kameran är från 2003 eller 2004. Den är ungefär 20 år gammal och det är oklart om den har USB […] Den är ganska gammaldags och krånglig att använda, vilket är frustrerande […]."* (R3)

Andra enheter som är föråldrade inom sjukvården är personalens arbetstelefoner. Respondenterna menar att arbetstelefonerna som används är analoga knapptelefoner som är tjugo år gamla. R3 berättar att dessa knapptelefoner är för omoderna: *"[...] det handlar om*

knapptelefoner. De är cirka 20 år gamla eller något liknande." Detta får medhåll från R5 men som ändå tycker att dessa arbetstelefoner fungerar bra till att dela patientdata på ett snabbt och säkert sätt: "*[…] vi hanterar patientdata främst via jobbtelefon, vilket känns säkrare. Men det känns ändå lite gammaldags. Dock fungerar det för att få jobbet gjort snabbt och säkert."*

En annan arbetsprocess som används är att man använder fax för att skicka remisser. Det finns lagar på att denna metod måste användas när man vill skicka över patientdata till ett annat sjukhus. R3, R4 och R7 menar dock att faxa patientdata är en föråldrad metod som är väldigt tidskrävande och de är tveksamma till om det verkligen är ett bra och säkert tillvägagångsätt för att skicka känslig information:

> "*Att använda fax istället för digitala system är en process som genererar mycket papper och är ineffektivt [...] I vården är det fortfarande vanligt att faxa, trots dess långsamma och föråldrade teknik […].* " (R3)

> " *[…] vi använder fortfarande fax eftersom det finns lagar som kräver en specifik hantering av patientuppgifter men där finns det jättemycket som kan utvecklas."* (R4)

> *"Att faxa tar onödigt lång tid och det är relativt lätt för utomstående att komma åt den informationen vilket blir en patientsäkerhetsrisk."* (R7)

4.2.2 Tidskrävande arbetsverktyg

Samtliga respondenter berättar att stationära arbetsdatorer används i det dagliga arbetet. Dessa datorer är väldigt långsamma på att starta upp alla program om man loggar in med sina egna inloggningsuppgifter, något som R7 tar upp: *"Vårt arbete är inte genomförbart om man ska sätta sig och logga in på datorn varje gång eftersom hårdvaran är alldeles för långsam[...]."* Detta får medhåll från R5 som även tar upp att man använder flera olika datorer under ett arbetspass och det går inte att sitta och vänta på datorerna ska starta upp när man måste utföra sitt arbete:

> " *[…] datorn tar 10 minuter på sig att logga in varje gång och du ska byta mellan 5 olika datorer under en ett arbetspass. Du kan liksom inte sitta en timme och vänta på att datorerna ska komma igång när du har massa andra saker att göra […]."* (R5)

4.3 Workarounds inom sjukvården

Samtliga respondenter påpekar att användningen av workarounds förekommer dagligen, främst för att sjukvården använder sig av omoderna digitala system och verktyg. Detta leder

till att man använder sig av alternativa lösningar för att effektivisera sitt arbete. R2 menar att workarounds har utvecklats till en kultur inom sjukvården. Alternativa lösningar lärs ut och det är så man ska arbeta, speciellt vid hanteringen av varningsrutor i systemen: "*[...] det känns som kulturen är att rutor ska klickas bort. För det är så man gör och man baserar det mycket på att andra har gjort det tidigare. Om man frågar vad det är för ruta så säger någon att den kan vi klicka bort, så det är på den nivån."*

4.3.1 Olika typer av workarounds i det dagliga arbetet

Flertalet respondenter nämner att de använder olika typer av workarounds i sitt dagliga arbete, och en vanligt förekommande workaround är den som används vid hanteringen av medicinsk fotografering. Det korrekta arbetssättet är att använda sjukhusets egna digitalkamera och ladda upp bilder i journalsystemet. R2 påpekar dock att systemen tenderar att krångla: "*[...] det tar en evighet att ladda upp bilden, och när det väl är gjort kan det även krångla för läkaren på nästa sjukhus att ladda ner bilden. Trots att man går igenom hela processen är det frustrerande att det ändå strular, vilket tvingar oss att skicka bilder på andra sätt."* Även R5 påpekar att det uppstår problem med användningen av sjukhusets digitalkamera och att man hellre hittar en snabbare lösning: "*[...] det kan ta över ett dygn att få in bilderna av en akut sjuk patient som du behöver ha snabb hjälp med bedömning på. Då kan jag verkligen förstå varför man tar fram sin mobiltelefon för att kunna skicka bilden direkt och få en snabbare lösning för att kunna hjälpa patienten."*

En annan workaround som används inom sjukvården är att det skrivs upp inloggningsuppgifter på post-it lappar som sätts på stationära datorer runt hela sjukhuset. Ett annat problem som förekommer är att man inte låser datorerna när man går ifrån dem. De lämnas obevakade och vem som helst skulle kunna gå dit och få tillträde till sjukvårdens program och information. R5 och R7 berättar:

> *"Vi använder generella inloggningsuppgifter till de stationära datorerna över hela sjukhuset. Eftersom läkare jobbar på flera olika avdelningar så kan man inte komma ihåg lösenorden till alla datorer så då står användarnamn och lösenord på kanten av datorn så att alla enkelt kan logga in. Dessa datorer finns tillgängliga för alla [...]."* (R5)

> *"[...] vi låser aldrig våra datorer när vi går in till patienterna så vem som helst kan gå förbi vår expedition och använda datorn [...] skärmlåset går igång först efter 15-30 minuter."* (R7)

4.3.2 Workarounds som livräddande lösning

Det framkommer att flera respondenter använder workarounds för att det är hjälpa patienter snabbare men att det i sin tur kan leda till att man tummar på IT-säkerheten. Läkares syfte är att rädda patienter och det är viktigare att patienten får rätt vård och behandling än att det uppstår en IT-säkerhetsmässig konsekvens. R5 berättar att "*[...] läkare ser syftet med att vi måste hjälpa någon. Vi måste göra någonting som kanske är jättebråttom och då måste vi göra det som funkar och inte det som kanske är det bästa IT-säkerhetsmässigt alltid."* Även R3 anser att patientens hälsa kommer i första hand: "*[...] vi gör det för att vinna tid och för att kunna ge patienter rätt typ av vård. Jag tror inte någon läkare står och tänker att nu bryter jag mot våra IT-säkerhetsregler utan mer att jag måste handlägga patienten på ett bra sätt."*

Ibland under en kritisk situation krävs det snabba, lösningsorienterade beslut för att hitta livräddande lösningar. Då använder läkare sig av lösningar som kan bryta eller underminera sjukhusets och patientens IT-säkerhet. R1 och R4 ger exempel på där man kan behöva använda sig av dessa lösningar:

> *"Ibland är det direkt livräddande för patienten att man väljer och dela information utanför de etablerade och tillåtna vägarna. Det kan göra att man snabbare hittar rätt diagnos och inleder rätt behandling."* (R1)

> *"Till exempel, om vi står inför en situation där en patient har hjärtstopp och vi behöver skicka information till en erfaren expert någonstans så finns det ingen annan metod än att använda sin egna telefon för att filma och skicka det snabbt."* (R4)

4.4 Användning av personliga enheter inom sjukvården

Flera respondenter förklarar att personliga enheter är något som används till en hög grad i det dagliga arbetet på sjukhus. R1 menar att det kan till och med vara något som förväntas av till exempel äldre kollegor men också av arbetsgivare: " *[...] det finns en förväntan om att man ska vara med i olika chatgrupper för att kunna ta del av information. Det är den primära kontaktvägen man använder.*"

Vidare förklarar R2 att det finns en viss hierarki och att man som yngre läkare kan bli tillsagd av en senior kollega att använda sin personliga mobiltelefon för att skicka olika typer av information vidare: "*[…] framför allt för yngre läkare då det finns en viss hierarki och blir man tillsagd av en senior kollega, att man ska skicka saker via sin personliga telefon med sms*

eller liknande, då hamnar man i en knepig sits där liksom det enda alternativet är att göra saker som man inte riktigt vet om det är så man ska gå till väga."

I dagsläget vittnar samtliga respondenterna att personliga mobiltelefoner används relativt ofta för att ta kort på, till exempel hudutslag och benbrott. Det framkommer även att man filmar ultraljudsundersökningar. Det enda sättet att konsultera en ultraljudsundersökning med en kollega är att filma skärmen för att kunna dela informationen, något som R3 nämner:

> "*På akutmottagningen är det vanligt att vi använder våra personliga telefoner för att filma ultraljudsundersökningar eftersom det inte finns något annat effektivt sätt att spara dem. Om vi vill visa resultatet av en ultraljudsundersökning för en kollega för att kunna diskutera fynden i efterhand, så är det enda sättet att filma skärmen för att dela informationen*." (R3)

R5 förklarar att det även används för enklare uppgifter som att söka upp information när man som personal inte har nära till en arbetsstation.

> *" […] men man söker upp saker och man googlar och tittar på artiklar och sådana saker för att det var det lätt tillgängligt, så det tror jag att alla gör […]."* (R5)

4.4.1 IT-säkerhetsmedvetandet kring personliga enheter

Generellt är IT-säkerhetsmedvetenheten hos respondenterna relativt hög. Flera av respondenterna förklarar att man är medveten om att sjukhus har ett starkt hot mot sig från angripare. Det förekommer angrepp mot sjukhuset och system har legat nere någon gång den senaste tiden, något som R2 och R4 tar upp:

> "*[...] alltså det pågår angrepp hela tiden. Det är ju huruvida de lyckas med eller inte, och tittar man nationellt också så ser man hur många regioner och andra vårdgivare som har blivit utsatta."* (R2)

> *"Det har kommit olika mejl om att vi varit hackade. Jag vet att vårt labbsystem har varit hackat och det har varit olika sidor som har legat nere på grund av angrepp […]."* (R4)

Alla respondenterna blev tillfrågade om hur stor dem tror risken är att de själva blir utsatta för ett cyberangrepp. De flesta syftade på att risken är hög på grund av den starka hotbilden som finns mot sjukvården som nämnts ovan. Däremot påpekar R6 att risken för cyberangrepp är jätteliten och att man inte hade jobbat på det sättet med mobiltelefonen annars:

"*[…] Jag tror att den är jätteliten. För att annars har jag aldrig jobbat på det sättet som till exempel med att ta* kort." (R6)

Vidare förklarar R3, R5 och R6 att det finns situationer där man använder sig av personliga enheter trots att man är medveten om att det inte ligger i linje med IT-säkerhetsrutiner. Det förekommer att man fotograferar journaler och att man har bilder på patienter i sin personliga enhet. Man försöker avidentifiera bilderna genom att inte inkludera personnummer men ibland kan dessa ändå innehålla känslig information om patienter vilket är en allvarlig oro. Det finns en stor risk för läckage av patientdata vid detta tillvägagångsätt men det görs ändå av personal, främst för att effektivisera besvärliga arbetsrutiner men också för att det är det enda sättet.

"*Det är inte alltid självklart att ta en journal och gå till en kopieringsmaskin på röntgen eller på en annan avdelning. Därför väljer de flesta av oss att fotografera journalen utan patienter i bild. Under intensiva perioder kan jag ha ett betydande antal sådana bilder i min telefon, ibland flera dussin […] Ibland kan det hända att ett personnummer syns på bilden men då har jag beskurit bort det direkt efter att jag tagit den*." (R3)

"Att ta bilder med ens telefon och sedan ladda upp dem i molnet innebär en risk för läckage av information. Även om man avsiktligt försöker avidentifiera bilderna kan de fortfarande innehålla känslig information. Det ökar risken för obehöriga att få tillgång till informationen, vilket är en allvarlig oro." (R5)

" […] vi har ingen dedikerad enhet för att kunna göra det på något annat sätt, så då tar jag min egen telefon och så skickar jag via den." (R6)

4.4.2 Riktlinjer kring personliga enheters användning

En betydande insikt som framkommit från alla våra intervjuer är att respondenterna verkar ha begränsad kännedom om de exakta riktlinjer och policys som reglerar användningen av personliga enheter inom sjukvården. Detta indikerar en potentiell brist på klarhet eller kommunikation från sjukhusledningens sida när det gäller dessa riktlinjer. Nedan förklarar R6 att det kan finnas men att det är något som man aldrig har sett.

"Det är möjligt att det finns någon policy någonstans på någon internetsida, men det har jag aldrig sett." (R6)

Även R7 menar också på att det är oklart vad som gäller när det kommer till riktlinjer och policys kring avvändandet av personliga enheter*:" […] det står väl om det i anställningsavtalet som ligger ihop med sekretessfrågor om inte jag missminner mig. Vad som står i kan jag inte återge."*

5. Analys och diskussion

I detta avsnitt presenteras analys och diskussion av resultatet. Tidigare forskning kommer att fungera som grund för fortsatta resonemang. Avsnittets struktur är uppdelad i tre delar, Avsaknad av utbildning inom IT-säkerhet, Brister i digitala system leder till Workarounds samt Läkares erfarenheter av personliga enheter.

5.1 Ingen omfattande utbildning inom IT-säkerhet

Resultaten av denna studie påvisar att respondenterna inte har fått någon omfattande utbildning inom IT-säkerhet. I yrkesrollen som läkare arbetas det ofta under tidspress och andra mer väsentliga utbildningar för deras arbetsroll prioriteras. Många respondenter menar att de får väldigt många digitala utbildningar för att utvecklas som läkare och i brist på tid så nedprioriteras utbildningar för IT-säkerhet. De få utbildningar som har gjorts av läkare är enkla utbildningar som inte är anpassad efter målgruppen, där man som användare snabbt kan klicka sig igenom diverse steg för att kunna genomföra utbildningen. Med bristfällande utbildningsmaterial tillgängligt för personalen ökar även risken för tappad IT-säkerhetmedvetenhet för de anställda (Hepp m.fl., 2018; Wani m.fl, 2022). Det är väldigt viktigt att utbilda vårdpersonal för att öka medvetenheten om IT-säkerhet eftersom deras attityder gentemot IT-säkerhet är starkt kopplade till hur deras utbildning ser ut. Dessutom är det viktigt att kontinuerligt genomföra utbildningar inom organisationen för att säkerställa att personalen är väl informerad och håller sig uppdaterad i ämnet (Kang, Kang & Monsen, 2023). Vidare menar de att det är av stor betydelse att läkare erhåller lämplig utbildning inom IT-säkerhet. Det är avgörande för att förbättra deras förmåga att hantera IT-risker och hot för att säkerställa att patienters sekretess och integritet bevaras (ibid.)

Däremot upplevs IT-säkerhetsmedvetandet hög hos respondenterna då de förklarar vilka hot som de är exponerade för i deras dagliga arbete. Detta går i linje med Flores m.fl. (2023) som förklarar att IT-säkerhetsmedvetenheten är högre hos anställda idag än för några år sedan. Å andra sidan dyker det ständigt upp nya hot och möjligheter för angripare vilket ställer höga krav på att sjukhusledningen kontinuerligt erbjuder en uppdaterad IT-säkerhetsutbildning.

Som nämnt ovan så har flera respondenterna uttryckt ett behov för anpassad utbildning men även en mer motiverande utbildning. I dagsläget så har alla roller på sjukhusen samma IT-säkerhetsutbildning enligt respondenterna. I likhet med respondenterna påvisar Chowdhury, Katsikas och Gkioulos (2022) att anpassade IT-säkerhetsutbildningar är ett bra sätt att höja IT-

säkerhetsmedvetenheten hos de anställda. På så sätt kan man få optimala utbildningar till specifika roller och till en organisatorisk kontext, i detta fall bättre anpassade för läkare som arbetar inom sjukvården.

5.2 Brister i digitala system leder till Workarounds

Samtliga respondenter upplever att det finns brister i många av de digitala systemen som används idag inom sjukvården. Några system är utdaterade och inte anpassade för ny modern teknik medan andra system är för tidskrävande eller för upprepande. När det finns brister i befintliga digitala system så upptäcker läkare oftast ett sätt att kringgå dessa problem och använder sig av alternativa lösningar istället, så kallade workarounds. Detta får medhåll av Boonstra m.fl. (2021) som påpekar att workarounds används för att komma runt problem som finns i bristfälliga system. Respondenterna upplever även att de nuvarande systemen har kastats på dem och att de inte är designade för sjukvården. Många system har implementerats utan någon form av feedback från sjukvårdspersonalen och många avdelningar arbetar på olika sätt vilket leder till att systemen inte blivit optimerade för sjukvårdsmiljöer. Vid en offentlig upphandling finns det nog inte resurser till att träffa olika typer av läkare för att få en inblick i vilka funktioner som behövs. En tydlig konsekvens av detta är att respondenterna använder alternativa lösningar för att effektivisera sitt arbete vilket kan leda till betydande IT-säkerhetsrisker. Detta stämmer överens med vad Skyvell Nilsson, Törner och Pousette (2018) betonar, nämligen att när man utvecklar system är det viktigt att komma ihåg att vårdpersonalens huvudmål är patientens fysiska hälsa och välbefinnande. Därför är det avgörande att de som utvecklar systemen förstår att man måste ta hänsyn till sjukvårdpersonalens behov och intressen. Genom att få behovsanpassade system inom sjukvården kan sjukvårdspersonal förbättra vårdkvalitén och IT-säkerheten för patienter och sjukvården.

Pollini (2021) lyfter även fram att anställda använder sig av workarounds när system eller digitala enheter inte är tillräckligt användarvänliga. Detta är något som samtliga respondenter upplever. Det finns både system och enheter som knappt är användbara längre vilket leder till att man använder snabbare lösningar. Flertalet respondenter berättar att de tvingas använda personliga enheter vid medicinsk fotografering då det är för tidskrävande att hämta en gammal digitalkamera på andra sidan sjukhuset. Att använda personliga enheter ökar dock risken för dataintrång men detta tillvägagångsätt är ett måste ifall man vill förbättra effektiviteten av patientens vård (Wani, Mendoza & Gray, 2020). Respondenterna nämner

även andra arbetssituationer där workarounds förekommer, bland annat att man klickar bort varningsrutor för att komma åt journalsystem samt hanteringen av stationära datorer på sjukhuset. Några respondenter menar att man inte loggar ut från datorer när man lämnar dem obevakade samt att inloggningsuppgifter finns synliga på datorns bildskärm. Detta kan utgöra en stor säkerhetsrisk för patienters sekretess och integritet men det minimerar tidsförlusten för läkare som inte har tid att vänta på de långsamma digitala systemen. Wani, Mendoza och Gray (2020) påpekar att frekventa inloggningar kan upplevas som ett hinder i den dagliga verksamheten och att anställda gärna använder simplare lösningar för att spara tid. Det ses att sjukvården har fått en arbetskultur där IT-säkerheten nedprioriteras till förmån för att förbättra effektiviteten av läkares arbete och patienters vård. Det kan bli ett etiskt dilemma när läkare behöver hjälpa patienter snabbt samtidigt som man inte vill riskera att känslig patientdata hamnar i fel händer men samtliga respondenter framhäver att patienters fysiska hälsa alltid kommer i första hand.

5.3 Läkares erfarenheter av personliga enheter

Enligt respondenterna används personliga enheter dagligen inom sjukvården, speciellt mobiltelefoner. Flera respondenter menar på att det kan användas för att effektivisera och underlätta deras arbete. Enligt Wani m.fl. (2022) framhävs fördelarna med att använda personliga enheter inom sjukvården. En av fördelarna är att sjukvårdspersonalen kan förbättra sin effektivitet genom att använda sina egna enheter, som ofta är tillgängliga. Å andra sidan menar Nerminathan m.fl. (2017) på att det kan också innebära stora risker för sjukhusen vid användning av personliga enheter, BYOD är en stor risk till dataintrång då personliga enheter utsätter sjukvården för externa hot när det inte finns någon kontroll över vilka typer av enheter som används eller hur det ska användas av personalen (Wani m.fl., 2022).

Samtliga respondenter har varit osäkra kring riktlinjer och policys när det kommer till hur personliga enheter ska användas på arbetsplatsen. Flera respondenter nämner att det säkert finns på deras intranät eller på någon annan sida men det är ingen som vet helt säkert. När det inte finns tydliga riktlinjer kring hur de personliga enheterna ska användas tar läkare självständiga beslut gällande användningen av personliga enheter i sitt arbete. Detta gör att det kan bli svårt att bedöma balansen mellan de fördelar och risker som finns (Nerminathan m.fl, 2017). Wani m.fl. (2022) förklarar att riktlinjer och policys är kritiska för att öka IT-säkerheten gällande användandet av personliga enheter på sin arbetsplats. Med hjälp av detta kan sjukhusledningen införa riktlinjer för hur läkare använder sina personliga enheter och på

så sätt skydda patientdata och säkerställa IT-säkerheten för personliga enheter. I dagsläget är det möjligt att det redan finns riktlinjer och policys för läkare vid användning av personliga enheter, men det är inte något som kommuniceras ut av arbetsgivaren eller uppmärksammas enligt respondenterna.

IT-säkerhetsmedvetenheten kring användning av personliga enheter är hög hos respondenterna. Många är medvetna om att sjukhus har en stark hotbild för cyberangrepp, men att man frångår säkerhetsrutiner för att kunna effektivera sitt arbete. Som nämnt ovan så är det dock oklart vilka rutiner som finns eller vilka som faktiskt gäller, däremot nämner flera respondenter att man som läkare har någorlunda kunskap om vad som är okej och inte då juridik och patientsekretess ingår i deras utbildning. Trots de stora risker som finns med användning av personliga enheter inom sjukvården använder sig de flesta av respondenterna sig av detta för att effektivisera sitt arbete. Detta stöds av Wani m.fl. (2022) som beskriver att ineffektiva arbetsrutiner gör att vårdpersonal väljer att kringgå dessa arbetsrutiner med hjälp av personliga enheter trots att det finns risker med användningen.

6. Slutsats

Detta avsnitt ägnas åt att besvara studiens syfte och frågeställningar. Slutsatsen dras utifrån den tidigare presenterande analysen och diskussionen. Här presenteras även förslag för fortsatt forskning inom ämnet samt en kritisk reflektion över studiens genomförande.

I denna studie har syftet varit att utforska hur användningen av personliga enheter bland läkare inom sjukvården påverkar IT-säkerheten. Genom att analysera läkares attityder och erfarenheter kring Bring Your Own Device (BYOD) har vi fått en djupare förståelse för integrationen av sådana enheter i sjukvårdens arbetsflöde och dess påverkan på IT-säkerheten. Studien visar på läkares IT-säkerhetsmedvetenhet inom sjukvården är av avgörande betydelse för att säkerställa en trygg och effektiv användning av personliga enheter, genom att öka medvetenheten om potentiella IT-säkerhetsrisker och hot kan läkare bättre skydda både patientdata och sjukvårdssystem från cyberangrepp. Resultatet pekar på behovet av kontinuerlig IT-säkerhetsutbildning för läkare inom sjukvården. Genom regelbunden utbildning kan läkare hålla sig uppdaterade om de senaste säkerhetshoten och bästa praxis för att hantera dem, vilket i sin tur kan minska risken för dataintrång och säkerhetsincidenter. Även implementering av tydliga riktlinjer kring användning av Bring Your Own Device (BYOD) enheter är avgörande för att säkerställa en säker vårdmiljö. Genom att etablera klara regler och begränsningar för hur personliga enheter får användas inom sjukvården kan man minimera riskerna för oavsiktlig dataexponering och säkerhetsproblem. Studien betonar även vikten på investeringar i anpassade digitala verktyg för att stödja läkares arbete inom sjukvården. Genom att tillhandhålla säkra och effektiva digitala verktyg kan man underlätta arbetsflöden samtidigt som man säkerställer att patientdata skyddas på bästa möjliga sätt. Genom att adressera dessa aspekter kan sjukvården stärka sin IT-säkerhet och skapa en tryggare miljö för både personal och patienter. Fortsatt forskning och åtgärder inom dessa områden är av stor vikt för att möta de ökande utmaningar inom IT-säkerhet för sjukvården.

6.1 Förslag till fortsatt forskning

Under studiens gång har vi fått frågan om vi har sökt oss till fler läkare än den läkargrupp som blev tillfrågad att delta i studien. Detta för att respondenterna som deltog i vår studie är i någorlunda samma ålder, därför skulle det vara intressant att se om resultatet hade blivit annorlunda om man hade haft ett bredare åldersspann. Några respondenter menar att äldre läkares IT-säkerhetsmedvetenhet kopplat till personliga enheter kan vara något lägre så det öppnar upp för fortsatt forskning kring det och om det stämmer överens med läkarnas åsikter.

Det hade även varit intressant att göra en studie kring sjukhusledningens tillämpning av policys och riktlinjer kring användandet av Bring Your Own Device (BYOD), det vill säga vårdpersonalens personliga enheter. Det framkommer i tidigare forskning att mindre än hälften av alla sjukhus använder sig av BYOD-policys och i denna studie påpekar de flesta respondenterna att dem inte riktigt känner till om det finns några riktlinjer eller inte på detta specifika sjukhus. Den tidigare forskningen visar även att riktlinjer kring användandet av personliga enheter ses ha en avgörande roll för vårdpersonalens etiska användning av personliga enheter. Det öppnar upp för vidare forskning för att se hur det ser ut i verkligheten på detta sjukhus och hur sjukhusledningen tänker kring BYOD-policys för att säkerställa IT-säkerheten på sjukhuset.

Eftersom sjukvården är den bransch som är hårdast drabbad av cyberangrepp, skulle det vara värdefullt att genomföra en kvantitativ studie genom en enkätundersökning för att utvärdera hur IT-säkerhetsmedvetna läkare är inom sjukvården. Detta kan bidra till mer generella slutsatser kopplat till sjukvården över hela Sverige.

6.2 Kritisk reflektion

Nedanstående text är en kritisk reflektion som belyser möjligheterna att justera studiens design för att uppnå ett mer nyanserat resultat, baserat på författarnas nya insikter efter genomförandet av studien.

Att respondenterna har ungefär samma ålder och liknande teknikvana samt IT-säkerhetsmedvetenhet kan utgöra en begränsning för studiens generaliserbarhet och nyanserade resultat. Genom att begränsa urvalet till en homogen grupp riskerar forskningen att missa viktiga perspektiv och variationer som kan finnas inom andra åldersgrupper och tekniska erfarenhetsnivåer.

Avslutningsvis vill vi framhålla att vi är nöjda med resultatet av studien. Vi betonar att de tidigare diskuterade justeringarna som nämnts tidigare, sannolikt skulle ha haft en betydande inverkan på studiens resultat.

7. Referenser

Alkhaledi, R. & Hawamdeh, S. (2023). Electronic Health Records and Cyber Hygiene: A Qualitative Study of the Awareness, Knowledge, and Experience of Physicians in Kuwait. [Elektronisk] *Proceedings of the Association for Information Science & Technology*, vol. 60(1), ss. 21–30. Tillgänglig: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-03-15]

Alter, S. (2014). Theory of Workarounds. [Elektronisk] *Communications of the Association for Information Systems*, vol. 34. Tillgänglig: ScienceDirect [2024-03-18] DOI: 10.17705/1CAIS.03455

Argaw, S.T., Tronscoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.M., O'Leary, C., Eshaya-Chauvvin, B. & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. [Elektronisk] *BMC Medical Informatics and Decision Making*, vol 20, ss 1-10. Tillgänglig: Directory of Open Access Journals [2024-03-15] DOI: 10.1186/s12911-020-01161-7

Bellwood, P., Armstrong, B., S.Joe, R., Borycki, E. & Campbell, R. (2011). Educating Health Professionals about the Electronic Health Record (EHR): Removing the Barriers to Adoption. [Elektronisk] *Knowledge Management & E-Learning: An International Journa*l, vol 3(1), ss. 51–62. Tillgänglig: Directory of Open Access Journals [2024-03-15]

Boonstra, A., Jonker, T., Offenbeek, M. & Vos, J. (2021). Persisting workarounds in Electronic Health Record System use: types, risks and benefits. [Elektronisk] *BMC Medical Informatics & Decision Making*, vol. 21(1), ss. 1–14. Tillgänglig: Directory of Open Access Journals [2024-04-11]

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. [Elektronisk] *Qualitative Research in Psychology*, vol. 3(2), ss. 77-101. Tillgänglig: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-03-26]

Chang, L. Y. & Coppel, N. (2020). Building cybersecurityawareness in a developing country: Lessons from Myanmar. [Elektronisk] *Computers & Security,* vol. 97. Tillgänglig: ScienceDirect [2024-03-15] DOI: 10.1016/j.cose.2020.101959

Chowdhury, N., Katsikas, S. & Gkioulos, V. (2022). Modelling Effective Cybersecurity Training Frameworks: A Delphi Method-Based Study. [Elektronisk] *Computers and Security,* vol. 113. Tillgänglig: ScienceDirect [2024-02-06]. DOI: 10.1016/j.cose.2021.102551

Denscombe, M. (2018). Forskningshandboken: för småskaliga forskningsprojekt inom samhällsvetenskaperna. 4.uppl. Lund: Studentlitteratur

Deepa, S., Adresya Suresh, A., Nesma., Sajeev, J., Mahalakshmi, T. & Sheeba, K. (2024). Data mining for cyber biosecurity risk management – A comprehensive review. [Elektronisk] *In Computers & Security,* vol. 137. Tillgänglig: ScienceDirect [2024-03-15]. DOI: 10.1016/j.cose.2023.103627

Enisa (Europeiska byrån för nät- och informationssäkerhet) (2017). Stock taking of information security training needs in critical sectors. European Union Agency for Network and Information Security. Tillgänglig: https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors [2024-03-15]

Flores, C. V., Gonzalez, J., Kajtazi, M., Bugeja, J. & Vogel, B. (2023). Human Factors for Cybersecurity Awareness in a Remote Work Environment. [Elektronisk] *Proceedings of the 9th International Conference on Information Systems Security and Privacy ICISSP*, vol. 1, ss. 608–616. Tillgänglig: SwePub [2024-03-15]

Green, M.L. & Dozier, P. (2023). Understanding Human Factors of Cybersecurity: Drivers of Insider Threats. I *2023 IEEE International Conference on Cyber Security and Resilience (CSR).* 31 Juli, 2023, Venedig

Hepp, S., Tarraf, R., Birney, A. & Mubashir, A. (2018). Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. [Elektronisk] *Health Information Management Journal*, vol. 47, ss. 116-124. Tillgänglig: Academic Search Premier [2024-03-15] DOI: 10.1177/1833358317722038

Högskolan Väst (2024). *Regler för studenters behandling av personuppgifter.* Trollhättan: Högskolan Väst. Tillgänglig: https://www.hv.se/student/studier/rattigheter-skyldigheter/regler-for-studenters-behandling-av-personuppgifter/?sq=gdpr%20och%20examensarbeten [2024-03-26]

Javaid, M., Haleem, A., Ravi Pratap, S., & Rajiv, S. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. [Elektronisk]

Cyber Security and Applications, 1. Tillgänglig: Science Direct [2024-03-15] DOI: 10.1016/j.csa.2023.100016

Kang,P., Kang, J. & Monsen, K.A. (2022). Nurse information security policy compliance, information competence, and information security attitudes predict information security behavior. [Elektronisk] *Computers, Informatics, Nursing*, vol. 41(8), ss. 595–602. Tillgänglig: Supplemental Index [2024-03-15] DOI: 10.1097/CIN.0000000000000981

Koppel, R., Smith, S., Blythe, J. & Kothari, V. (2015). Workarounds to computer access in healthcare organizations: you want my password or a dead patient? [Elektronisk] *Stud Health Technol Inform,* vol. 208, ss. 215-220. Tillgänglig: PubMed [2024-03-18]

Mikuletič,S., Vrhovec, S., Skela-Savic,B. & Žvanut,B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. [Elektronisk] *In Computers & Security,* vol.136. Tillgänglig: Science Direct [2024-03-15] DOI: 10.1016/j.cose.2023.103489

MSB (Myndigheten för samhällsskydd och beredskap) (2020). Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden. Myndigheten för samhällsskydd och beredskap. Tillgänglig: https://www.msb.se/contentassets/fe72c449466e4017bd76787762ab9dc5/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf [2024-03-15]

MSB (Myndigheten för samhällsskydd och beredskap) (2024). Metoder vid cyberangrepp. Myndigheten för samhällsskydd och beredskap. Tillgänglig: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/risker-och-sarbarheter-inom-cybersakerhet-och-cyberfysiska-system/hot-och-metoder-inom-cybersakerhet/metoder-vid-cyberangrepp/ [2024-03-15]

Nerminathan, A., Harrison, A., Phelps, M., Scott, K.M. & Alexander, S. (2017). Doctors- use of mobile devices in the clinical setting: a mixed methods study. [Elektronisk] *Internal Medicine Journal*, vol. 47, ss. 291-298. Tillgänglig: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-03-15]

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E. & Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. [Elektronisk] *Sensors,* vol 21(15), ss. 5119. Tillgänglig: Directory of Open Access Journals [2024-03-15] DOI: 10.3390/s21155119

O'Brien,N., Ghafur, S., Durkin, M. (2021). Cybersecurity in health is an urgent patient safety concern: We can learn from existing patient safety improvement strategies to address it. [Elektronisk] *Journal of Patient Safety and Risk Management,* vol. 26. Tillgänglig: SageJournals [2024-03-15]

Patterson, E.S. (2018). Workarounds to Intended Use of Health Information Technology: A Narrative Review of the Human Factors Engineering Literature. [Elektronisk] *Human factors,* vol. 60 (3), ss. 281-292. Tillgänglig: MEDLINE [2024-03-18] DOI: 10.1177/0018720818762546

Pfleeger, C.P. (2015). Security in Computing. 5. Uppl. ; Pearson.

Pollini, A. Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. & Guerri, D. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. [Elektronisk] *Cognition, Technology & Work*, vol 24(2), ss. 371–390. Tillgänglig: APA PsycInfo [2024-03-15].

Ranganathan, V. (2016). BYOD done the smarter way. [Elektronisk] *Health Management Technology*, vol. 37(3), ss. 20–21. Tillgänlig: Medline [2024-03-15]

Skyvell Nilsson, M., Törner, M. & Pousette, A. (2018). Professional culture, information security and healthcare quality: an interview study of physicians' and nurses' perspectives on value conflicts in the use of electronic medical records. [Elektronisk] *Safety in health,* vol. 4. Tillgänglig: SwePub [2024-03-15] DOI:10.1186/s40886-018-0078-9

Soni, V., Kukreja, D. & Sharma, D. (2020). Security vs. Flexibility: Striking a Balance in the Pandemic Era. I 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). 14 December, 2020, New Delhi.

Säkerhetspolisen (2022). Cyberangrepp ständigt pågående hot mot Sverige. Säkerhetspolisen. Tillgänglig: https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2022-03-11-cyberangrepp-standigt-pagaende-hot-mot-sverige.html [2024-03-15]

Wani, T.A., Mendoza, A., Gray, K. & Smolenaers, F. (2022). Status of bring-your-own-device (BYOD) security practices in Australian hospitals – A national survey. [Elektronisk] *Health policy and technology*, vol. 11. Tillgänglig: British Library Document Supply Centre Inside Serials & Conference Proceedings [2024-03-15]

Wani, T.A., Mendoza, A. & Gray, K. (2020). Hospital Bring-Your-Own-Device Security Challenges and Solutions: Systematic Review of Gray Literature. [Elektronisk] *JMIR MHealht and UHealth*, vol 8. Tillgänglig: APA PsycInfo [2024-03-15]

8. Bilagor

Bilaga 1: Intervjuguide

Inledning

- Presentera oss själva och syftet med studien.
- Intervjun tar cirka 45 minuter och vi undrar om det är okej att den spelas in med både ljud och bild?
- Intervjun är frivillig och du kan när som helst välja att avbryta intervjun utan att behöva ge en förklaring till det.
- Allt material kommer att behandlas anonymt. Endast vi ansvariga har möjlighet att koppla svar till namn. Resultaten kommer att presenteras utan att avslöja några personers identitet, i sammanfattande form och med hjälp av illustrativa citat.
- Bekräfta att de ger sitt samtycke till att delta i studien och att resultaten publiceras

Bakgrundsfrågor

- Vad arbetar du med och kan du beskriva dina arbetsuppgifter?
- Hur ser en vanlig arbetsdag ut?
- Vilka var dina spontana tankar när vi berättade syftet med intervjun, att undersöka IT-säkerhet kopplat till personliga enheter? Använder du några personliga enheter, såsom egna telefoner eller datorer för arbetsrelaterade uppgifter?

Användning och erfarenhet av personliga enheter i arbetet

- Använder du några personliga enheter, såsom egna telefoner eller datorer för arbetsrelaterade uppgifter?
  - Hur använder du den personliga enheten? (T.ex. tar kort eller liknande)
  - Ur ett IT-säkerhetsperspektiv, ser du några risker med användningen av dessa personliga enheter?
- Har personalen fått tillåtelse av sjukvården att använda er av egna telefoner eller datorer i arbetet?
  -Om ja, varför tror du att ni får det?
  -Om nej, varför tror du personliga enheter används ändå?
- Finns det några rekommendationer personalen måste följa vid hanteringen av egna telefoner eller datorer?
- Hur upplever du den generella användningen av egna telefoner eller datorer inom sjukvården?
- Har sjukvården haft några IT-säkerhetsincidenter eller problem med egna telefoner eller datorer inom sjukvården? -Ge exempel
- Hur går ni tillväga idag för att dela känslig patientdata mellan personal?
- Ser du några för- eller nackdelar med detta arbetssätt?
- Finns det några särskilda utmaningar eller begränsningar med detta arbetssätt?

IT-säkerhet

- Finns det några riktlinjer eller policys inom sjukvården att jobba efter för att säkerställa IT-säkerheten?
- Har du fått någon utbildning inom IT-säkerhet i sjukvården?
  - Hur ofta har man denna utbildning?
  - Upplever du att utbildningen bidrar till en större medvetenhet om IT-säkerhet?
- Upplever du att utbildningar och tidigare erfarenheter ökar din förmåga att hantera hot? På vilket sätt?
- Vart skulle du vända dig om du misstänker att du blivit utsatt för ett cyberangrepp? (Rapportera incidenter?)
- Hur stor tror du risken är att du blir utsatt för ett cyberangrepp?
  - Varför tror du risken är stor/liten?
- Känner du att du har samma förmåga att hantera säkerhetsrisker och hot när du arbetar under stress?

Workarounds (Alternativa lösningar som används för att kringgå ett problem i befintliga arbetsrutiner)

- Kan du ge exempel på situationer där workarounds har använts för att kringgå IT-säkerhetsåtgärder inom sjukvården?
- Vad tror du är orsaken till att vårdpersonal använder workarounds?
- Vilka konsekvenser tror du att användningen av workarounds för IT-säkerhet kan ha för sjukvården och patienters säkerhet?
- Tycker du att användningen av workarounds effektiviserar ditt dagliga arbete?
- Tror du implementering av bättre digitala verktyg inom sjukvården kan minska behovet av att använda workarounds?

Avslutning

- Är det något du vill tillägga som vi inte har tagit upp under intervjun?
- Tacka för intervjun

Bilaga 2: Inbjudan till intervju

Hej *Namn på mottagare*, vi heter Joachim Åhlström och Magnus Uskali, vi är två studenter på Högskolan Väst och genomför vårt examensarbete som handlar om användningen av personliga enheter och IT-säkerhet inom sjukvården.

Vi skulle vilja börja med att tacka för att vi fick delta i ert tidigare möte där vi fick en inblick hur ni använder personliga enheter samt hur ni tänker kring säkerhetsaspekterna. Vi är mycket intresserade av dina erfarenheter och synpunkter, och vi skulle vilja bjuda in dig till en digital intervju för att få en djupare förståelse för ämnet.

Vår studie syftar till att utforska användningen av personliga enheter inom sjukvården och dess påverkan på IT-säkerhet. Intervjun beräknas ta cirka 45 minuter och kommer att spelas in och transkriberas för att säkerställa noggrann dokumentation.

Ditt deltagande i intervjun är helt frivilligt, och du kan när som helst välja att avbryta deltagandet utan att behöva ge någon förklaring. Vi vill också informera om att allt insamlat material behandlas konfidentiellt, och endast vi som är ansvariga för studien kommer att kunna koppla dina svar till ditt namn. Resultaten kommer att presenteras anonymt i sammanfattande form och med illustrativa citat.

Vi ber dig vänligen bekräfta att du ger ditt samtycke till att delta i vår studie och informera oss om när det passar för en intervju. Har du inte möjlighet att delta, så vidarebefordra gärna mailet och inbjudan till en kollega.

HÖGSKOLAN VÄST

Institutionen för ekonomi och IT

461 86 TROLLHÄTTAN

Tel 0520-22 30 00

www.hv.se