Secify

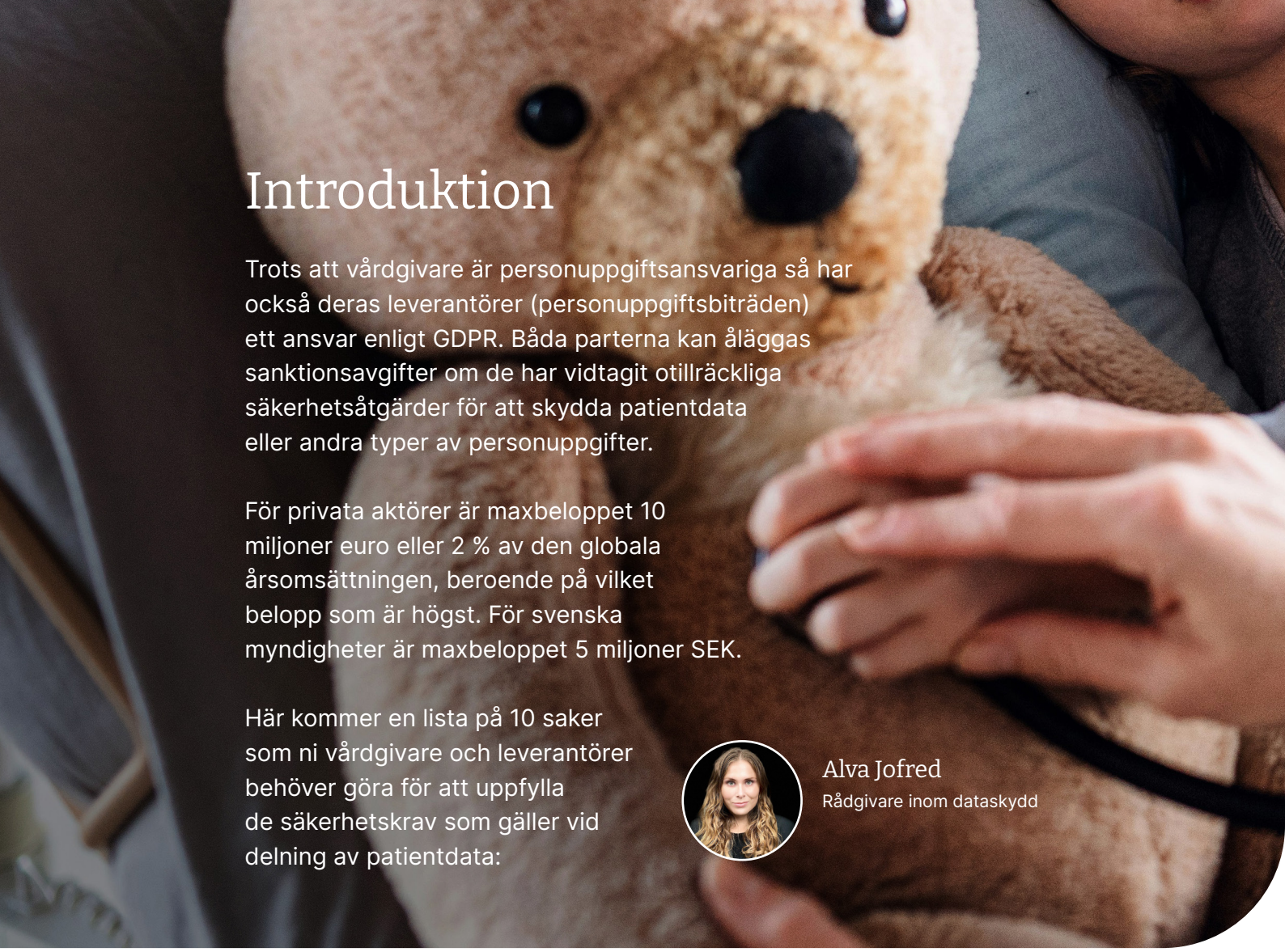
Checklista

Säker kommunikation

10 åtgärder för att säkra upp din delning av patientdata

“ Med gemensamt ansvar hanterar vi patientdata för att forma en framtid av trygghet och tillit, där varje handling är ett steg mot en säkrare värld.

- Alva Jofred



Introduktion

Trots att vårdgivare är personuppgiftsansvariga så har också deras leverantörer (personuppgiftsbiträden) ett ansvar enligt GDPR. Båda parterna kan åläggas sanktionsavgifter om de har vidtagit otillräckliga säkerhetsåtgärder för att skydda patientdata eller andra typer av personuppgifter.

För privata aktörer är maxbeloppet 10 miljoner euro eller 2 % av den globala årsomsättningen, beroende på vilket belopp som är högst. För svenska myndigheter är maxbeloppet 5 miljoner SEK.

Här kommer en lista på 10 saker som ni vårdgivare och leverantörer behöver göra för att uppfylla de säkerhetskrav som gäller vid delning av patientdata:

Alva Jofred
Rådgivare inom dataskydd

Checklistan

- ☐ Se till att ni har personuppgiftsbiträdesavtal som dels uppfyller alla krav i GDPR, dels gör det tydligt för er vilka säkerhetsåtgärder som ska vidtas när patientdata delas eller på andra sätt hanteras.
- ☐ Om ni vill kommunicera med eller om patienter digitalt, se till att patientdatan krypteras. Här är det viktigt att ni kontinuerligt beaktar teknikutvecklingen, så att vald krypteringslösning vid var tid utgör ett reellt skydd mot obehörig åtkomst.
- ☐ Om ni vill kommunicera med eller om patienter digitalt, se till att patientdatan endast kan nås genom stark autentisering. Exempel på metoder för stark autentisering är BankID, Freja eID och SITHS-kort.

- ☐ Nu när ni vet vilka säkerhetskrav som gäller när ni delar patientdata via öppna nät. Utforma rutiner som gör det enkelt för alla medarbetare att skicka och ta emot patientdata på ett säkert sätt. Det ska vara lätt att göra rätt, och svårt att göra fel.

- ☐ Ta fram utbildningar för att säkerställa att alla medarbetare känner till aktuella säkerhetskrav, följer verksamhetens rutiner och förstår konsekvenserna av eventuella överträdelser. Medarbetarna bör även regelbundet få information om nya lagar och riktlinjer på området.

- ☐ Om ni önskar skicka pseudonymiserade patientdata till t.ex. AI- och forskningsaktörer i förhoppningen om att patientdatan inte längre räknas som personuppgifter om mottagaren inte kan återidentifiera dessa; sitt lugnt i båten. Avvakta tills vi har mer praxis och vägledning på området. Förhoppningsvis har vi snart ett prejudicerande avgörande från The European Court of Justice i mål T-557/20.

- ☐ Av praktiska skäl är det under vissa förutsättningar tillåtet för vårdgivare att skicka påminnelser och kallelser via sms eller e-post. Om ni vill göra detta, se till att ni:

  1) Har gjort en behovs- och riskanalys,
  2) Har inhämtat patientens aktiva samtycke,
  3) Ser till att sms/mejl-texten inte innehåller några detaljer om patientens hälsotillstånd eller andra personliga förhållanden. Här är det mycket viktigt att ni tar hänsyn till vilken typ av verksamhet ni bedriver. Det är skillnad på att skriva ”Välkommen till ditt besök inom Region Stockholm” och att skriva ”Välkommen till ditt besök på HIV-mottagningen”. Den sistnämnda texten avslöjar detaljer om patientens hälsa, medan den förstnämnda inte gör det. Av säkerhetsskäl är det bäst om ni sköter all kommunikation via en säker e-tjänst. Eventuella påminnelser

och kallelser via sms eller e-post (som alltså skickas helt oskyddat) behöver då inte innehålla mer specifik information än något i stil med: ”Hej, du har ett nytt meddelande i Tjänsten X. Logga in med BankID på TjänstenX.se för att läsa meddelandet”.

- ☐ Tänk på att patientdata inte får delas via exempelvis sms eller e-post ens om patienten själv önskar det. Patienten kan inte samtycka till att dennes personuppgifter hanteras på ett sätt som strider mot dataskyddslagstiftningen (t.ex. GDPR och HSLF-FS 2016:40).
- ☐ Vårdgivare – Säkerställ att era personuppgiftsbiträdesavtal alltid innehåller en klausul som gör det möjligt för er att granska era leverantörer, göra inspektioner och få tillgång till all information som behövs för att kontrollera att leverantören lever upp till sina skyldigheter enligt avtalet och dataskyddslagstiftningen.
- ☐ Vårdgivare – Följ regelbundet upp era befintliga leverantörer. Ta gärna fram checklistor och riktlinjer som underlättar granskningarna.

Secify