



## Informationssäkerhet

Detta dokument ger en grundläggande bild av vad systematiskt informationssäkerhetsarbete innebär, vilket ska bedrivas i alla vårdverksamheter. Dokumentet tar också upp vikten av säker nätverksanvändning när det kommer till patientsäkerhet. I kombination med patientdatalagen är dessa fundamentala att ta hänsyn till vid distansarbete med känsliga personuppgifter, som också tas upp i dokumentet.

### Systematiskt informationssäkerhetsarbete

En vårdgivare ska utföra ett systematiskt informationssäkerhetsarbete. Grundläggande innebär detta enligt tredje kapitlets 2 § i *Socialstyrelsens föreskrifter och allmänna råd (HSLF-FS 2016:40) om journalföring och behandling av personuppgifter i hälso- och sjukvården*, att säkerställa följande:

1. Dokumenterade personuppgifter hos vårdgivaren ska vara åtkomliga och användbara för den som är behörig (tillgänglighet).
2. Att personuppgifterna är oförvanskade (riktighet).
3. Att obehöriga inte kan ta del av personuppgifterna (konfidentialitet).
4. Att åtgärder kan härledas till en användare (spårbarhet) i informationssystemet/journalsystemet.

Informationssäkerhetsarbetet går alltså fundamentalt ut på att vårdgivaren säkrar att tillgängligheten, riktigheten, konfidentialiteten och spårbarheten uppfylls när det gäller verksamhetens journalsystem. För att möjliggöra detta ska en informationssäkerhetspolicy upprättas. Detta framgår av tredje kapitlets 4 § i *Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården*, vilken lyder som följer:

4 § Vårdgivaren ska ansvara för att det finns en informationssäkerhetspolicy. Den ska ange vårdgivarens övergripande mål för och inriktning på verksamhetens arbete med informationssäkerhet i syfte att säkerställa personuppgifternas tillgänglighet, riktighet, konfidentialitet och spårbarhet.

En informationssäkerhetspolicy kan förslagsvis innehålla följande:

- Varför är det viktigt med informationssäkerhet?
- Hur uppnås informationssäkerhet?
- Vem bär ansvar för vad inom informationssäkerheten?
- Vem bär ansvar för policyn?
- Hur ses policyn över och revideras.

### Internätverk och patientsäkerhet

Internätverk och informationssystem spelar en allt viktigare roll i vården och höga krav ställs på säkerheten i dessa system så att patientsäkerheten bibehålls. Tillgängligheten till informationssystemen och att den information om patienterna som finns i dessa är korrekt och tillförlitlig, är avgörande för att patienterna ska få en god och säker vård i rätt tid. Om



säkerheten i nätverk och informationssystem brister, kan det leda till allvarliga patientsäkerhetsrisker, samt att känsliga uppgifter om patienter röjs och kommer i orätta händer.

Inspektionen för vård och omsorg (IVO) granskar säkerhet i nätverk och informationssystem inom hälso- och sjukvården. Syftet är att säkerställa ett en hög nivå på säkerheten i nätverk och informationssystem upprätthålls. Ytterst handlar det om patientsäkerhet. IVO samverkar med andra myndigheter och har även byggt upp sin interna kompetens och utvecklat metoder för tillsyn. Myndigheten gör dokumentgranskningar, men utför även digitala och fysiska tillsyner.

### Distansarbete och känsliga personuppgifter

Med anledning av covid-19-pandemin så har de som har möjlighet att arbeta hemifrån, uppmanats att så göra i så stor utsträckning som möjligt. På många arbetsplatser har detta blivit en rutin som kommit för att stanna. Att hantera tidböcker och granska röntgenbilder, är exempel på arbetsuppgifter som tekniskt sett kan utföras på annan plats än tandvårdskliniken. Men även om det är möjligt att utföra vissa av de arbetsuppgifter som ingår i en tandvårdsverksamhet på distans, så ska det beaktas att man hanterar känsliga personuppgifter och *patientdatalagens* (2008:355) syfte ska upprätthållas. Syftet framgår av det första kapitlets 2 §, vilken lyder som följer:

1. Informationshantering inom hälso- och sjukvården ska vara organiserad så att den tillgodoser patientsäkerhet och god kvalitet samt främjar kostnadseffektivitet.
2. Personuppgifter ska utformas och i övrigt behandlas så att patienters och övriga registrerades integritet respekteras.
3. Dokumenterade personuppgifter ska hanteras och förvaras så att obehöriga inte får tillgång till dem.

Vidare framgår av sjätte kapitlets 1 § i *Socialstyrelsens av föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården*, att hälso- och sjukvårdspersonal ska ansvara för att:

1. Personliga lösenord och hjälpmedel för autentisering inte kan bli tillgängliga för annan.
2. Datorer eller andra enheter som används för att hantera uppgifter om patienter inte lämnas utan att uppgifterna är skyddade mot obehörig åtkomst.

Detta ska vara utgångspunkten även då arbetsuppgifter utförs hemifrån. Därtill ska verksamhetens informationssäkerhetspolicy följas och de nätverkssystem som används, ska vara säkra. MSB flaggar för att det är av yttersta vikt att alla företag har tydliga riktlinjer som alla medarbetare har god kännedom om gällande distansarbete.