Ansvarig	Upprättad av	Berörda verksamheter	Fastställt datum
Verksamhetschef HSL	MAS	Hälsa och omsorg	2025-12-08,rev 2026-08-05
Dokumentnamn Rutin för hantering av sekretessbrott, dataintrång och loggkontroller	**Ledningssystem** Enligt SOSFS 2011:9		**Diarienummer**

Innehållsförteckning

1. Allmänt

Enligt lag är vårdgivaren skyldig att skydda patienters personuppgifter, förebygga sekretessbrott och dataintrång samt att återkommande kontrollera att obehöriga inte tar del av elektroniskt dokumenterade patientuppgifter - så kallade loggkontroller.

Endast den personal som är involverad i patientens vård och i behov av journaluppgifter för att kunna utföra sitt arbete får ha tillgång till dessa.

2. Syfte

Att säkerställa så misstänkta eller bekräftade sekretessbrott och dataintrång och upptäckta via loggkontroller i elektroniska system utförs för att säkerställa att patienternas integritet respekteras och att dataskyddslagar följs.

Rutinen gäller för samtlig personal som hanterar personuppgifter eller annan känslig information i digitala system.

3. Information till personalen

Personal som ska hantera patientuppgifter i digitala system eller på annat sätt ska få information av anställande chef enligt nedan:

- Rutin för hantering av sekretessbrott, dataintrång och loggkontroller
- Egenansvar för att endast ta del av de uppgifter som arbetet kräver
- Att loggkontroller utförs regelbundet
- Hur följderna vid en incident gällande olovlig hantering av patientuppgifter hanteras
- Att obehörig åtkomst kan leda till rättsliga åtgärder

Ansvaret gäller chefer som anställer legitimerad personal samt chefer som anställer vårdpersonal som utför vårdåtgärder på uppdrag av legitimerad personal och då räknas som hälso- och sjukvårdspersonal.

4. Loggkontroller på den enskildes eller legal företrädares begäran

En patient eller legal företrädare kan begära ut loggutdrag över vem som tagit del av dennes personuppgifter. Ansvarig chef gör en prövning om loggarna kan lämnas ut. Lista på loggkontroller för den tidsperiod och det urval som begärts ut lämnas till systemförvaltare. I informationen ska det framgå i vilka IT-system patientens personuppgifter finns registrerade, vilken verksamhet och vid vilka tidpunkter någon tagit del av uppgifterna.

Uppgifterna lämnas ut via rekommenderat brev till folkbokföringsadressen eller kan hämtas ut efter uppvisande av legitimation.

Begäran om loggutdrag dokumenteras i patientjournalen.

5. Åtkomstkontroller - loggkontroller

Loggkontroller utförs för att kontrollera vem som läst, ändrat eller skrivit ut information från olika system.

Exempel på händelser att uppmärksamma vid loggkontroller är:

- Avsaknad av vårdrelation: Åtkomst till patientuppgifter utan vårdrelation.
- Ovanliga åtkomsttidpunkter: Inloggning eller läsning av journaler vid tidpunkter som avviker från ordinarie arbetstid.
- Hög åtkomstfrekvens: Omfattande läsning eller aktivitet i ett ärende som inte motsvarar behovet för aktuell vårdinsats.
- Åtkomst till inaktiva ärenden: Läsning i ärenden som inte är aktuella eller är avslutade.
- Personliga kopplingar: Åtkomst till uppgifter om släktingar, närstående eller kollegor
- Profilpersoner: Patienter som är allmänt kända i samhället, lokalt eller nationellt.
- Särskilt känsliga medicinska uppgifter: Avser patienter med medicinska uppgifter som bedöms vara ovanliga eller extra integritetskänsliga
- Ingen åtkomstfrekvens: Berörd medarbetare är inte aktiv i patientjournalen enligt gällande rutin för dokumentation.

5.1 Systematiska kontroller

Utförs på samma sätt varje gång enligt ett beslutat schema

System	Systemansvarig	Frekvens	Omfattning	Kontrollerar loggar
Treserva Hälsoärende	Caroline Svensson	Varannan månad	20 medarbetare	Ansvarig chef
APPVA	Caroline Svensson	Varje månad	Samtliga verksamheter	Ansvarig chef
Nationell Patient Översikt (NPÖ)	Caroline Svensson	Varje månad		Ansvarig chef
Mina Planer	Caroline Svensson	Varje månad		Ansvarig chef
Nationell läkemedelslista	Ola Svensson	2 ggr/år		Ansvarig chef
EVONDOS	Ola Svensson	2ggr/år		Ansvarig chef
Pascal	Nina Danicic	2ggr/år		Ansvarig chef

5.2 Slumpmässiga kontroller

Utförs vid behov i kombination med de systematiska kontrollerna

Kontroll	Frekvens	Beslutas av	Kontrollerar loggar
Loggar till utvald patient	1 ggr/år, vid behov	Vc HSL, MAS, SF, AC	Berörd chef
Avvikande tider på dygnet	1 ggr/år, vid behov	Vc HSL, MAS, SF, AC	Berörd chef
Profilpersoner	Vid intervall för systematiska kontroller	Berörd Ec informerar Vc HSL, MAS, SF eller AC	Berörd chef
Särskilt känsliga medicinska uppgifter	Vid behov	EC, VC HSL, MAS, SF, AC	Berörd chef
Patienter med skyddade patientuppgifter	Vid intervall för systematiska kontroller	Berörda chefer informerar Vc HSL, MAS eller SF	Berörd chef
Loggar på utvald personal då berörd chef misstänker olovlig aktivitet i systemet	Vid behov	Berörda chefer informerar Vc HSL, MAS, SF eller AC	Berörd chef
DF	Vid behov	Berörda chefer informerar Vc HSL, MAS, SF eller AC	Berörd chef

5.3 Kontroller efter begäran

Begärs ut efter behov

System	Systemansvarig	Frekvens	Kontroll av loggar
ExorLive	Christina Nordström	Efter behov	Berörd chef
My-Loc	Christina Nordström	Efter behov	Berörd chef
Sesam LMN	Nina Danicic	Efter behov	Berörd chef
Svenska palliativregistret	Nina Danicic	Efter behov	Berörd chef
BPSD	Nina Danicic	Efter behov	Berörd chef

6. Dokumentation av loggkontroller

Systemförvaltare skickar ut underlag för loggkontroller till berörda chefer. Berörd chef kontrollerar loggar och dokumenterar resultat efter fastställda mallar.

Kontrollerade loggar samt ifylld mall skickas tillbaka till systemförvaltare för förvaring och gallras efter fem år.

7. Vid misstanke om överträdelse

Vid misstanke om sekretessbrott, dataintrång eller avvikelse i loggkontroller ska händelsen utredas av ansvarig chef. Medarbetare informeras om möjligheten att ta med facklig företrädare till mötet för utredning.

Utredningen dokumenteras fortlöpande efter fastställd mall. Tidpunkter, beskrivning av händelse samt inblandade personer samt upprättade åtgärder med tidsplan ska finnas i dokumentationen. Utredningen skrivs under av ansvarig chef och medarbetare. Originalet förvaras i personakten. Medarbetaren får en kopia.

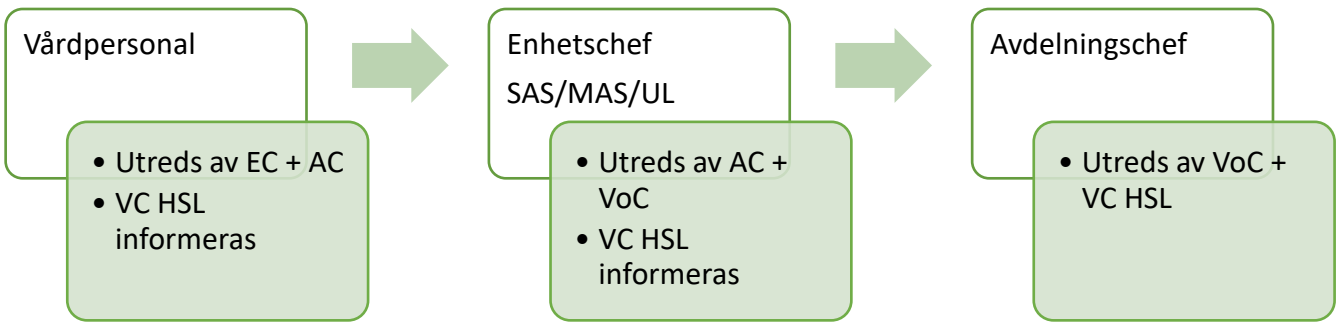
7.1 Åtgärder vid bekräftad incident

- Skydda bevismaterial som loggar, e-post eller annan systemdata
- Informera kommunens dataskyddsombud
- Vid dataintrång och sekretessbrott: Kontakta HR för disciplinära åtgärder och verksamhetschef HSL för beslut om polisanmälan

7.2 Rapportering

- Vid dataintrång enligt GDPR rapport till Integritetsskyddsmyndigheten (IMY) inom 72 timmar
- Berörda individer ska informeras om att deras uppgifter röjts

Incidenterna hanteras av berörd chefer enligt schema:



8. Uppföljning och förbättringsåtgärder

Incidenten utreds och analyseras även enligt rutin för avvikelsehantering för att upprätta eventuella förbättringsåtgärder för att förhindra upprepning.