Rutiner för rapportering av personuppgiftsincident

Denna rutin avser att utgöra en översikt av incidentrapporteringsprocessen i enlighet med regelverket i nya dataskyddsförordningen (General Data Protection Regulation, GDPR) som fr.o.m. den 25 maj 2018 ersatte personuppgiftslagen (PUL).

Incidentrapportering

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

En personuppgiftsincident ska rapporteras av sjukhuset till tillsynsmyndigheten (Datainspektionen) inom 72 timmar efter det att överträdelsen har upptäckts. Därför måste det finnas rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter skyndsamt.

Vid rapportering ska personuppgiftsincidenten beskrivas, sannolika konsekvenser, ungefärligt antalet berörda registrerade samt vilka åtgärder som vidtagits och/eller föreslås att vidtas.

Process för incidentrapportering

Vid händelse av personuppgiftsincident ska närmaste chef informeras och incidenten ska rapporteras till sjukhusets IT:s incidentorganisation utan dröjsmål. För nationella kvalitetsregister där sjukhuset är registeransvarig ska registerhållaren även informeras om incidenten.

Mallen för rapportering av en personuppgiftsincident, sist i detta dokument, ska användas vid rapporteringen av en personuppgiftsincident.

Incidenten rapporteras sedan vidare utan dröjsmål från IT:s incidentorganisation till sjukhusets juristavdelning för vidare hantering. SMS ska samtidigt skickas till juristavdelningen för att uppmärksamma att ett mail har skickats om en personuppgiftsincident.

Sjukhusets juristavdelning initierar samma dag eller nästkommande ordinarie arbetsdag en utredning. Om personuppgiftsincidenten bedöms vara av sådan karaktär att den ska anmälas ska anmälan diarieföras innan den anmäls till Datainspektionen.

Juristavdelningen avgör efter samråd med sjukhusets informationssäkerhetssamordnare och berörda verksamhetschefer eller registerhållare om incidenten kräver att sjukhuset måste informera de registrerade om incidenten.
Som personuppgiftsansvarig anmäler sjukhuset personuppgiftsincidenten inom 72 timmar till tillsynsmyndigheten (Datainspektionen). En anmälan ska åtminstone innehålla följande (Art. 33 GDPR):

- Personuppgiftsincidentens art
- Ungefärligt antalet berörda registrerade
- Kontaktuppgifter på Dataskyddsombudet samt andra viktiga kontakter för incidenten

- Beskriva sannolika konsekvenserna av incidenten
- Beskriva de åtgärder som vidtagits eller föreslås att vidtas för att åtgärda och mildra incidenten

Den formella anmälan vidarebefordras till ansvariga chefer för berörda verksamheter för att säkerställa att anmälda åtgärder vidtas och uppföljning sker av incidenten.
För kvalitetsregister sker denna rapportering till berörd registerhållare.

Mall för rapportering av en personuppgiftsincident

Vid händelse av personuppgiftsincident ska närmaste chef informeras och incidenten ska rapporteras till sjukhusets IT:s incidentorganisation utan dröjsmål. För nationella kvalitetsregister där sjukhuset är registeransvarig ska registerhållaren även informeras om incidenten.

Vid rapportering ska nedanstående uppgifter lämnas:

Kontaktuppgifter på den som rapporterar:	*Namn, Titel, Enhet, Telefonnummer, Email m.m*
Närmaste chef och/eller verksamhetschef:	*Namn, Titel, Enhet, Telefonnummer, Email m.m*
Personuppgiftsincidentens art:	*Beskriv personuppgiftsincidentens art och vad som hänt.*
Antalet berörda registrerade:	*Uppskatta antalet individer som är berörda av incidenten.*
Konsekvenser av incidenten:	*Beskriv sannolika konsekvenser av incidenten.*
Åtgärder gjorda och/eller föreslås:	*Beskriv de åtgärder som vidtagits eller föreslås att vidtas för att åtgärda och mildra incidenten.*