Håndtering av lagringsmedia (faktaark 34)

Versjon 3.2

01.10.2018

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket omhandler sikker håndtering av lagringsmedia som brukes til lagring av helse- og personopplysninger. Formålet med faktaarket er å sikre konfidensialitet for helse- og personopplysninger. IKT-ansvarlig skal sikre korrekt håndtering av lagringsmedia. Regler og prosedyrer skal etableres før behandling av helse- og personopplysninger starter. Omfatter alle lagringsmedia som inneholder helse- og personopplysninger. Med lagringsmedia menes bl.a. harddisk, tape, CD, minnepinne, osv.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er virksomheter som behandler helse- og personopplysninger og som benytter seg ulike typer lagringsmedia for lagring av helse- og personopplysninger. Faktaarket er relevant for personer som skal vurdere om virksomhetens behandling av helse- og personopplysninger oppfyller de grunnleggende kravene i personvernforordningen. Dette vil ofte være personer som er tildelt et særlig ansvar for personvern i virksomheten.
Krav i Normen	Faktaarket gjelder følgende kapitler i Normen • Kapittel 5.3 Fysisk sikkerhet og håndtering av utstyr • Kapittel 5.3.3 Infrastruktur
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Personvernforordningen artikkel 32. Sikkerhet ved behandlingen

Håndtering av lagringsmedia

Nr.	Handling/Utførelse
1	**Merking av lagringsmedia** a) Virksomheten skal ha oversikt og føre hendelsesregister som viser hvilke lagringsmedia som benyttes til å lagre helse- og personopplysninger (se eksempel på hendelsesregister under) b) I tilfeller hvor alle lagringsmedia i virksomheten behandles under ett (lagringsmedia som inneholder og som ikke inneholder helse- og personopplysninger) er det ikke nødvendig med merking av det enkelte lagringsmedium, men kun sikre at alle behandles korrekt (oppbevaring, forsending, rekonstruksjon, sletting) c) Enkeltvis skal lagringsmedium merkes med for eksempel ”Inneholder pasientdata” eller ”Inneholder pasientjournal” d) Merkingen plasseres på et godt synlig sted
2	**Oppbevaring av lagringsmedia** a) Lagringsmedia som inneholder helse- og personopplysninger skal oppbevares avlåst i serverrom eller på annen måte (låst skap, bankboks, osv)
3	**Forsendelse av lagringsmedia** a) Lagringsmedia som inneholder helse- og personopplysninger skal sendes som rekommandert post
4	**Rekonstruksjon av eller service på lagringsmedia hos ekstern leverandør** a) Flyttes lagringsmedia fra virksomheten eller databehandler for rekonstruksjon eller service skal det opprettes en avtale mellom virksomheten og ekstern leverandør. Avtalen skal sikre konfidensialitet og at ekstern leverandør sletter alle helse- og personopplysninger etter at oppdraget er avsluttet b) Virksomheten kan ikke overføre lagringsmedia som inneholder helse- og personopplysninger til land utenfor EU, med mindre den registrerte gir samtykke eller overføringen er godkjent av Datatilsynet c) Register over lagringsmedia oppdateres for å vise hvor alle lagringsmedia til enhver tid er
5	**Avhending av lagringsmedia** a) Ved avhending av lagringsmedia som inneholder helse- og personopplysninger (i server eller PC, mobilt utstyr, tape, osv) skal dette behandles slik at det ikke er fare for brudd på krav til konfidensialitet b) Lagringsmedia som avhendes skal slettes slik at det ikke er mulig å gjenskape helse- og personopplysninger. Det anbefales at slettingen utføres av en ekstern leverandør som skal slette lagringsmedia med sletteløsning godkjent av Nasjonal Sikkerhetsmyndighet (NSM) c) Alternativt til sletting er at lagringsmedia fysisk demonteres og ødelegges (brenne eller makulere minneplatene/-enhetene i lagringsmediet) d) Register over lagringsmedia må oppdateres for å dokumentere status på lagringsmedia

Eksempel på register over lagringsmedia

Nr	Type	Innehold	Merking	Oppbevaring / Plassering	Status
1.	Harddisk	Pasientjournal	Server er merket med ”Inneholder pasientjournal”	Avlåst i serverrom	I bruk
2.	Harddisk	Pasientjournal	Server er merket med ”Inneholder pasientjournal”	Slettet og avhendet 15. mai 2007	Slettet av <navn på ekstern leverandør>
3.	Backuptape	Pasientjournal	Tape er merket med ”Inneholder pasientjournal”	Avlåst i bankboks	I bruk

Eksempelet er ikke utfyllende og viser f.eks. ikke SAN-løsninger hvor data lagres utenfor server i sentrale lagringsløsninger. Slike løsninger dekkes av pkt 1 b) over.