

   	Utgitt med støtte av: 
Norm for informasjonssikkerhet www.normen.no	
<h2 style="text-align: center;">Fysisk sikring av områder og utstyr</h2>	Støttedokument Faktaark nr 17 Versjon: 3.1 Dato: 20.09.2018

Formål	Hindre uautorisert adgang til utstyr benyttet for behandling av helse- og personopplysninger. Faktaarket omhandler kun fysisk sikring av utstyr lokalisert i en virksomhet. Elektronisk sikring er ikke inkludert. Mobilt utstyr og hjemmekontor er heller ikke inkludert.		
Ansvar	Det overordnede ansvaret ligger hos virksomhetens ledelse, mens gjennomføring av dem er vanligvis delegert til medarbeidere i virksomheten.		
Gjennomføring	Ved behandling av helse- og personopplysninger.		
Omfang	<ul style="list-style-type: none"> • Alle virksomheter i helsesektoren skal ha tiltak for å hindre at uautoriserte får fysisk adgang til helse- og personopplysninger. • Den fysiske sikringen gjelder både for utstyr benyttet for å behandle helse- og personopplysninger og annet utstyr med betydning for informasjonssikkerheten. • Tiltakene for fysisk sikring av områder og utstyr skal være tilpasset virksomhetens størrelse og hvor det behandles helse- og personopplysninger. 		
Målgruppe	<input type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input checked="" type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input checked="" type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
Dette faktaarket er spesielt relevant for			
Hjemmel	Personvernforordningen artikkel 32		
Referanser	Norm for informasjonssikkerhet, kapittel 5.3		

Merknad 20.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Beskrivelsene nedenfor er eksempler på tiltak som kan gjennomføres for å hindre uautorisert adgang til utstyr. For å sikre at tiltakene er tilpasset den enkelte virksomhets behov og trusselbilde, bør alle de ulike områdene som er beskrevet i dette faktaarket vurderes og tiltak identifiseres gjennom en risikovurdering..

I likhet med at en PC med helse- og personopplysninger sikres med f.eks. autentiseringsløsning, brannmur, tilgang etter behov, er det av like stor betydning at fysisk sikring ivaretas. Brudd på den fysiske sikkerheten til områder og utstyr vil øke faren for at uvedkommende får tilgang til elektronisk lagrede helse- og personopplysninger. Det er et samspill mellom tiltak for den fysiske sikringen og tiltak som er iverksatt for elektronisk sikring. Tiltakene er gjensidig avhengig av hverandre for at en skal kunne oppnå tilfredsstillende sikring av helse- og personopplysninger.

Nr.	Aktivitet/Beskrivelse
1.	Risikovurdering a) Risikovurderingen må ta utgangspunkt i de konkrete fysiske arealene som skal sikres mot uautorisert adgang, se Faktaark 7 – Risikovurderinger b) Risikovurderingen bør belyse behov for å definere arealene i ulike soner, ut fra virksomhetens størrelse. En sonemodell for fysisk adgang til helse- og personopplysninger for interne og eksterne kan defineres slik: <ul style="list-style-type: none"> – Åpen sone: arealer hvor publikum har fri adgang, korridorer, venterom, fellesarealer, områder med alminnelig ferdsel – Indre sone: åpne arbeidsplasser (områder med begrenset ferdsel), arealer beregnet kun for medarbeidere i virksomheten, evt. publikum i følge med medarbeidere - resepsjonsarbeidsplassen, kontorer, vaktrom, behandlingsrom

Nr.	Aktivitet/Beskrivelse
	<ul style="list-style-type: none"> – Sikker sone: areal hvor kun spesielt godkjente medarbeidere har adgang, og hvor publikum ikke skal ha adgang (områder med sterk adgangsbegrensning), datarom, rom med nettverk, servere og kommunikasjonsutstyr c) For mindre virksomheter der soneinndeling ikke er mulig må risikovurderingen belyse risiko for adgang til helse- og personopplysninger innen det aktuelle arealet
2.	<p>Nøkler/adgangskort</p> <ul style="list-style-type: none"> a) Identifiser områder og rom hvor utstyr med helse- og personopplysninger er plassert b) Lag en oversikt over hvem som har tjenstlige behov for adgang til aktuelle områder og rom. Adgang til dedikerte rom med driftsutstyr (servere og utstyr) skal kun gis til personell med absolutt behov for adgang. Generelt skal adgang i størst mulig grad begrenses. c) Lag en kvitteringsliste for tildeling av nøkler/adgangskort. Alle som får utlevert og leverer inn nøkler/adgangskort skal kvittere med navn, sted og dato for utleveringen/innleveringen. Listen bør revideres f.eks. 1 gang i året, evt. hyppigere når adgangene ofte endres. d) I større virksomheter anbefales det en egen resepsjonstjeneste. Uautorisert personell og besøkende skal ledsages
3.	<p>Besøk av eksterne til eller via områder og rom hvor utstyr med helse- og personopplysninger er plassert</p> <ul style="list-style-type: none"> a) Etabler resepsjonstjeneste og/eller ledsagelse av uautorisert eksterne personer (besøkende) b) Skrivere og arbeidsstasjoner som er plassert i tilknytning til fellesområder (resepsjoner, venterom, vaktrom, korridorer mv.) fysisk sikres slik at uvedkommende ikke får adgang til helse- og personopplysninger
4.	<p>Adgang til driftsutstyr (data- og kommunikasjonsrom)</p> <p>Sikkerhetstiltak skal hindre at annet enn autorisert personell får adgang til slikt utstyr</p> <ul style="list-style-type: none"> a) Mindre virksomhet: Servere og annet nettverksutstyr skal oppbevares i låst skap eller rom med sylindrelås. Dersom det benyttes et skap, skal dette skrues fast til veggen eller gulvet. Skapet skal ikke plasseres i resepsjonen/publikumsområde. Resepsjon/publikumsområde skal heller ikke benyttes som rom for oppbevaring av utstyret. b) Større virksomhet: Alle servere og annet nettverksutstyr skal oppbevares i et eget datarom, fortrinnsvis med kodelås. Det skal også være installert et system for varsling av innbrudd, som skal være tilkoplek kodelåsen. Systemet skal varsle en ansvarlig for datarommet, alternativt vaktentral. Det kan vurderes å etablere en egen vaktordning. c) Adgang til data- og serverrom bør registreres. F.eks. kan det føres en oversikt, hvor alle besøk registreres med navn, leverandør, oppdragsbeskrivelse, dato, tid for inn og ut, og servicemedarbeiderens signatur.
5.	<p>Medisinsk teknisk utstyr</p> <ul style="list-style-type: none"> a) Lagringsenhet for medisinsk teknisk utstyr som behandler helse- og personopplysninger skal plasseres i avlåst rom eller i bemannet område. b) Medisinsk teknisk utstyr som behandler helse- og personopplysninger skal inkluderes i virksomhetens arbeid med informasjonssikkerhet, herunder risikovurderinger, adgangsregulering, fysisk sikring og prosedyrer for bruk, på linje med andre informasjonssystemer.

Når det gjelder sikring av bærbart utstyr og hjemmekontor, se Faktaark 18 – Sikring av bærbart utstyr og Faktaark 29 – Hjemmekontor.