Vedlegget er à jour med versjon 6.0 av Normen.

Kravtabellen er strukturert iht tabellen nedenfor og er iht innholdsfortegnelsen i Normen.

| Område | Delområde |
| --- | --- |
| A. Ledelse og ansvar | 1. Roller og ansvar for informasjonssikkerhet og personvern
2. Dataansvarliges ansvar
3. Databehandlers ansvar
4. Styringssystemet
5. Ledelsens gjennomgang
 |
| B. Risikostyring | 1. Forholdsmessighet ved valg av tiltak
2. Minimumskrav for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet
3. Oversikt over teknologi og behandling av helse- og personopplysninger
4. Risikovurdering og risikohåndtering
5. Vurdering av personvernkonsekvenser
 |
| C. Grunnleggende om behandling av helse- og personopplysninger | 1. Behandlingsgrunnlag
2. Plikter og krav ved behandling av helse- og personopplysninger
3. Innebygd personvern
 |
| D.Informasjonssikkerhet | 1. Medarbeidere, kompetanse og holdningsskapende arbeid
2. Tilgangsstyring
3. Fysisk sikkerhet og håndtering av utstyr
4. Sikker IT-drift
5. Kommunikasjonssikkerhet
6. Digital kommunikasjon til den registrerte
7. Leverandørforhold og avtaler
8. Håndtering av informasjonssikkerhetsbrudd
9. Nødrutiner
 |

### Bruk av kravtabellen

Kravtabellen er utformet med tanke på gjennomføring av sikkerhetsrevisjoner. Den kan også brukes i andre sammenhenger der det trengs en systematisk oversikt over Normens krav. Eksempler på dette kan være i anskaffelser, for en leverandør til å vise samsvar eller i revisjon og utvikling av et system.

##### Forklaring til innholdet i kravtabellen nedenfor:

**Krav**

Kravtabellen inneholder krav med ”skal” i Normen slik at det på en enkel måte er mulig å verifisere om virksomheten følger Normen. Alle spørsmål skal besvares med ”Ja” for at kravet skal være oppfylt. Det anbefales å bruke kravtabellen sammen med Normen slik at kravet vurderes ift temaet som behandles i Normen.

Virksomheten skal vurdere hvilke krav fra Normen som gjelder basert på den konkrete behandlingen av personopplysninger (jf. Normen kap 3.1)

##### Kap. i Normen

Referanse til kapittelnummer i Normen.

##### Kap. i ISO 27001

Referansene er iht ISO 27001 – 2017 og ISO 27001 – 2017 Annex A.

Spesielt om A.18.1: Annex A: viser til at «alle relevante lovfestede, regulatoriske og kontraktsmessige krav samt organisasjonens tilnærming til å oppfylle disse kravene skal være uttrykkelig identifisert og dokumentert», men uten å spesifisere disse kravene nærmere. Dette kravet i ISO er ikke tatt med i lista. Det utløses automatisk dersom kravet i Normen har hjemmel i lov/forskrift. Hvis en virksomhet mener å oppfylle A.18.1, bør det verifiseres at Normens spesifikke krav på dette området etterleves.

\* = Kravet i Normen er delvis dekket av ISO 27001. Det vil si at kravene i Normen er mer konkrete og utdypende enn kravene i ISO 27001. I disse tilfellene er dette markert med en \* bak kapittelnummeret.

(A.X.X\* & A.Y.Y\*) = A.X.X og A.Y.Y er hver for seg delvis dekkende for kravet i Normen. Disse to kravene vurderes til sammen å utgjøre fullstendig samsvar med det aktuelle kravet i Normen, som er synliggjort ved bruk av parentes og skilletegnet "&".

##### Systemkrav i behandlingsrettet helseregister

Angir sikkerhetskrav som skal ivaretas i systemer som behandler helse- og personopplysninger (tidligere Faktaark 38). For noen krav er det angitt eksempler på sikkerhetskrav til systemer som ikke direkte kan leses ut av Normen. Disse er angitt som ”Eksempler på sikkershetskrav:”.

##### Kravet gjelder ikke helt eller delvis for virksomheten (Må begrunnes)

Normen bygger på prinsippet om forholdsmessig sikring. Ved bruk av kravtabellen må virksomheten derfor avgjøre hvilke spørsmål som er relevante, og foreta konkrete avveininger i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv. Bortfaller kravet må dataansvarlig redegjøre for hvorfor kravet utgår.

##### Er kravet ivaretatt?

Kryss av om kravet er ivaretatt eller ikke.

##### Hjemmel til kravet i lov eller forskrift

Der det er hjemmel i lov- eller forskrift for kravet, er hjemmelen angitt i kolonnen. Det betyr ikke at hjemmelen dekker hele virksomhetens behandling eller aktiviteter. F.eks. dersom hjemmelen er Pasientjournalloven og virksomhetens behandling/ aktivitet ikke faller inn under lovens virkeområde, vil ikke dette være en relevant hjemmel. Dette må virksomheten vurdere selv.

Følgende akronymer for hjemmel er benyttet i tabellen:

* EFF: Eforvaltningsforskriften (<https://lovdata.no/dokument/SF/forskrift/2004-06-25-988>)
* FEP: Forskrift om etablering og gjennomføring av psykisk helsevern (§49) (<https://lovdata.no/dokument/SF/forskrift/2011-12-16-1258>
* FIKT: Forskrift om IKT-standarder i helse- og omsorgstjenesten (<https://lovdata.no/dokument/SF/forskrift/2015-07-01-853>)
* FLK: Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten (<https://lovdata.no/dokument/SF/forskrift/2016-10-28-1250>)
* HFL: Helseforskningsloven (<https://lovdata.no/dokument/NL/lov/2008-06-20-44>
* HPL: Helsepersonelloven (<https://lovdata.no/dokument/NL/lov/1999-07-02-64>
* HTL: Helse- og omsorgstjenesteloven (<https://lovdata.no/dokument/NL/lov/2011-06-24-30>)
	+ Med utgangspunkt i hva et forvaltningsorgan er, vurderes forskriften som relevant for kun enkelte virksomheter i sektoren (jf jusinfo.no: *Forvaltningsloven gjelder etter § 1 for ”den virksomhet som drives av forvaltningsorganer “ (offentlig virksomhet), når ikke annet er bestemt i eller i medhold av lov. Et forvaltningsorgans virksomhet omfattes også av forvaltningsloven, når forvaltningen ikke fatter vedtak og utøver offentlig myndighet, dvs. når handlingen ikke anses for å være ”bestemmende for rettigheter eller plikter” og dermed ikke er ”utøvelse av offentlig myndighet”. Forvaltningen er således i all sin virksomhet underlagt de lovfestede og ulovfestede regler om offentlig saksbehandling, også når ikke myndighet eller vedtakskompetanse utnyttes.”* og Wikipedia *”I Norge er forvaltningsorgan typisk regjeringen, departementene, direktorater, fylkeskommuner og kommuner. Kommunestyre og fylkesting regnes også gjerne med.”* )
* HTIL: Helsetilsynsloven (<https://lovdata.no/dokument/NL/lov/2017-12-15-107>)
* PBL: Pasient- og brukerrettighetsloven (<https://lovdata.no/dokument/NL/lov/1999-07-02-63>)
* PJF: Pasientjournalforskriften (<https://lovdata.no/dokument/SF/forskrift/2019-03-01-168>)
* PJL: Pasientjournalloven (<https://lovdata.no/dokument/NL/lov/2014-06-20-42>)
* POL: Personopplysningsloven (<https://lovdata.no/dokument/NL/lov/2018-06-15-38>)
* PVF: Personvernforordningen (GDPR) (<https://lovdata.no/dokument/NL/lov/2018-06-15-38>)

##### Kravet blir ivaretatt av databehandler

Kolonnen kan benyttes til å markere om kravet blir ivaretatt av databehandler. For krav som ikke kan overlates til databehandler er feltet grået ut.

Krav som både dataansvarlig og databehandler skal ivareta er markert med grønt.

**Samlet oversikt Normens krav**

| Nr | Krav (formulert som spørsmål) | Kap. i Normen | Kap. i ISO 27001 og Annex A | Systemkrav i behandlings-rettet helse-register | Kravet gjelder ikke helt eller delvis for virksomheten(Må begrunnes) | Er kravet ivaretatt? | Hjemmel til kravet i lov eller forskrift | Kravet blir ivaretatt av data-behandler |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Er valg av egnede tekniske og organisatoriske tiltak vurdert i forhold til virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 1.5 | 6.1.18.1  |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 6 |  |
|  | Er valgte tiltak basert på risikovurderinger? | 1.5 | 6.1.38.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PVF artikkel 35 (1)PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er valgte tiltak forholdsmessige ift virksomhetens størrelse og omfanget av behandling av personopplysninger? | 1.5 | 6.1\*8.1.\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PVF artikkel 35 (1)PJL § 22HRL § 21 |  |
|  | Sørger virksomhetens øverste leder for virksomheten at gjeldende krav til informasjonssikkerhet og personvern følges? | 2 | 5.15.25.3  |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21HTL § 5-10 første punktumPVF artikkel 24FLK § 7 |  |
|  | Har virksomhetens øverste leder bestemt nivå for akseptabel risiko? | 23.2 | 6.1.2 |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32FLK § 5 og 6 | [ ] Ja [ ] Nei |
|  | Har virksomhetens øverste leder bestemt regler for håndtering av risiko? | 2 | 6.1.3 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PLF § 6 | [ ] Ja [ ] Nei |
|  | Har virksomhetens øverste leder sørget for velfungerende styring og kontroll? | 2 | 6.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 24 første leddFLK §§ 3 og 4PLF § 7 | [ ] Ja [ ] Nei |
|  | Er alle tiltak dokumentert | 2 | 6.1.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 5 nr. 2 og 32PJL §§ 22 og 23HRL § 21 | [ ] Ja [ ] Nei |
|  | Har virksomhetens øverste leder sørget for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver for å ivareta ansvaret? | 2.1 | 5.3 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23PVF artikkel 24 første leddFLK § 7 | [ ] Ja [ ] Nei |
|  | Er det tydelig hvem som er ansvarlig, og hva de er ansvarlig for? | 2.1 | 5.3 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23PVF artikkel 24 første leddFLK § 7 | [ ] Ja [ ] Nei |
|  | Er alle kjent med hvilke oppgaver de har? | 2.1 | 5.3 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23PVF artikkel 24 første ledd | [ ] Ja [ ] Nei |
|  | Har alle tilstrekkelig kunnskap om andres relevante ansvar og oppgaver? | 2.1 | 5.3 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23PVF artikkel 24 første ledd | [ ] Ja [ ] Nei |
|  | Er alle kjent med hvem som har myndighet til å ta beslutninger? | 2.1 | 5.3 |  |  | [ ] Ja [ ] Nei | PJL § 23PVF artikkel 24 første ledd | [ ] Ja [ ] Nei |
|  | Har øverste leder utpekt personvernombud når virksomheten er offentlige virksomheter og i privat virksomhet når informasjonsbehandlingens omfang, art og formål krever det? | 2.1 | 5.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 37 (1) | [ ] Ja [ ] Nei |
|  | Blir personvernombudet gitt tilstrekkelige ressurser og tilgang på aktuell kompetanse til å utføre sine plikter? | 2.1 | 7.1\*7.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 38 (2) | [ ] Ja [ ] Nei |
|  | Arbeider personvernombudet uten interessekonflikt med eventuelle andre roller som vedkommende innehar i virksomheten, og mottar ikke instruksjoner vedrørende hvordan oppgavene skal utføres? | 2.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 38 (3) (6) | [ ] Ja [ ] Nei |
|  | Har virksomheten etablert et styringssystem for informasjonssikkerhet og personvern (internkontroll)? | 2.4 | 4.4 |  |  | [ ] Ja [ ] Nei | PJL § 23PVF artikkel 24 første ledd | [ ] Ja [ ] Nei |
|  | Er styringssystemet tilpasset virksomhetens størrelse, risiko, egenart og aktiviteter og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i? | 2.4 | 4.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 24 og 32 | [ ] Ja [ ] Nei |
|  | Har øverste ledelse gjort styringssystemet kjent i virksomheten?  | 2.4 | 5.1 |  |  | [ ] Ja [ ] Nei | FLK §§ 3 og 7(d) | [ ] Ja [ ] Nei |
|  | Gir øverste ledelse tilstrekkelige økonomiske rammer og ressurser for gjennomføring av nødvendige aktiviteter? | 2.4 | 7.1 |  |  | [ ] Ja [ ] Nei | PJL § 23 | [ ] Ja [ ] Nei |
|  | Er styringssystemet dokumentert? | 2.4 | 7.5.1 |  |  | [ ] Ja [ ] Nei | PJL § 23PVF artikkel 5 nr. 2 og 24 første leddFLK § 3 og 5 | [ ] Ja [ ] Nei |
|  | Blir dokumenter i styringssystemet holdt løpende oppdatert og arkivert fra det tidspunktet dokumentet ble erstattet med en ny gjeldende versjon? | 2.4 | 7.5.2 |  |  | [ ] Ja [ ] Nei | FLK § 5 (3) | [ ] Ja [ ] Nei |
|  | Vurderer dataansvarlig om detaljert informasjon, som kan ha sikkerhetsmessig betydning, skal fjernes før utlevering eller ved deling med annen virksomhet? | 2.4 | A.8.2.3\* |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23 2. ledd | [ ] Ja [ ] Nei |
|  | Blir dokumentasjon av risiko og tiltak knyttet til informasjonssikkerhet sikret ut fra de behov for sikkerhet som foreligger? | 2.4 | 7.5.3 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23 2. ledd | [ ] Ja [ ] Nei |
|  | Er dokumentasjon av risiko og tiltak til enhver tid oppdatert og tilgjengelig? | 2.4 | 8.28.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 24, 1.FLK § 5 | [ ] Ja [ ] Nei |
|  | Når virksomheten er offentlige virksomheter er det beskrevet mål og etablert strategi for informasjonssikkerhet? | 2.4 | 6.2 |  |  | [ ] Ja [ ] Nei | EFF § 15 (1) |  |
|  | Gjennomgår øverste ledelse virksomhetens aktiviteter innen informasjonssikkerhet og personvern minst en gang i året? | 2.5 | 9.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 24, 1.FLK § 8 | [ ] Ja [ ] Nei |
|  | Vedtas det tiltaksplaner, med tidsfrister og plassering av ansvar, om gjennomgangen avdekker at virksomhetens risikonivå ikke er akseptabelt? | 2.5 | 9.3 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22FLK § 6 | [ ] Ja [ ] Nei |
|  | Dokumenteres ledelsens gjennomgang?  | 2.5 | 9.3 |  |  | [ ] Ja [ ] Nei | PJL § 23PVF artikkel 5 nr. 2HRL § 22FLK § 5 | [ ] Ja [ ] Nei |
|  | Har virksomheten etablert egnede tekniske og organisatoriske tiltak som er egnet for å håndtere risiko på en tilfredsstillende måte? | 3 | 6.1.3 |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32 (1)(b) | [ ] Ja [ ] Nei |
|  | Er tiltakene for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet i informasjonssystemene balanserte? | 3 | 6.1.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Blir det tatt hensyn til den tekniske utviklingen, gjennomføringskostnadene og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i, når et akseptabelt risikonivå vurderes? | 3 | 6.1.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 (1) | [ ] Ja [ ] Nei |
|  | Tas det hensyn til for eksempel type og mengde opplysninger, virksomhetens størrelse og behandlingens kompleksitet i arbeidet med risikostyring? | 3 | 6.1.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 (1) | [ ] Ja [ ] Nei |
|  | Velges og vurderes egnede tekniske og organisatoriske tiltak opp mot virksomhetens art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv? | 3.1 | 6.1.1\*8.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Sørger virksomheten for at det er forholdsmessighet mellom risiko og tiltakets kostnad? | 3.1 | 6.1.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Har virksomheten fastsatt nivå for akseptabel risiko basert på Normens minimumskrav til informasjonssikkerhet og eventuelt egne informasjonssikkerhetsmål? | 3.2 | 6.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32EFF § 15 | [ ] Ja [ ] Nei |
|  | Er følgende minimumskrav til konfidensialitet fastsatt?:Virksomheten skal ivareta taushetsplikten og for øvrig sikre mot at uvedkommende får kjennskap til opplysninger. * hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
* avgrense tilgang for autorisert personell iht. tjenstlig behov
* ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerhet
 | 3.2 | (A.9.2\*,A.10.1\*,A.11.1\*,A.11.2\*,A.12.4\*&A.13.2.4\*) |  |  | [ ] Ja [ ] Nei | PJL §§ 15, 19, 22HPL § 21, 21 aPJF § 14PVF artikkel 5 nr. 1 f | [ ] Ja [ ] Nei |
|  | Er følgende minimumskrav til integritet fastsatt?:Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er sikret mot utilsiktet eller uautorisert endring eller sletting.* logge hvem som har foretatt registrering, endring, retting og sletting
* hindre utilsiktet eller uautorisert endring eller sletting
* sikre at helse- og personopplysninger registreres på rett person
* sikre at helse- og personopplysninger føres i henhold til relevant kodeverk og terminologi
* sikre at helse- og personopplysninger er korrekte og om nødvendig oppdaterte
* hindre at kopier av data blir en kilde til utdatert informasjon
 | 3.2 | A.12.4\*A.9.2\* A.9.4.1\*A.12.3\* |  |  | [ ] Ja [ ] Nei | PJL § 22PJF § 14PVF artikkel 5 nr. 1 f, PVF art 32 nr. 1 bokstav b | [ ] Ja [ ] Nei |
|  | Er følgende minimumskrav til tilgjengelighet og robusthet fastsatt?:Virksomheten skal sikre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er tilgjengelig til rett tid.* sikre at helse- og personopplysninger er tilgjengelig iht. tjenstlig behov
* sikre forsvarlig og stabil drift av informasjonssystemene
* sikre at det finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting
* sikre at informasjonssystemene er tilgjengelig iht. virksomhetens tilgjengelighetskrav
 | 3.2 | (A.9.2\*,A.12.1\*,A.12.4.1\*,A.17.1\*&A.17.2\*) |  |  | [ ] Ja [ ] Nei | PJL § 19, 1. leddPJL § 22PJF § 14, 3. leddPVF artikkel 5 nr. 1 f, PVF 32 nr. 1 bokstav b og c? | [ ] Ja [ ] Nei |
|  | Behandles brudd på kravene til konfidensialitet, integritet, tilgjengelighet og robusthet som avvik? | 3.2 | A.16.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 33 | [ ] Ja [ ] Nei |
|  | Har virksomheten utarbeidet protokoll over behandlinger av helse- og personopplysninger | 3.3 | A.8.1.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 30 |  |
|  | Har virksomheten oversikt over IKT-systemer, infrastruktur, digitale tjenester og annen informasjon med betydning for informasjonssikkerheten, mv.? Oversikten bør være dokumentert | 3.3 | A.8.1.1 |  |  | [ ] Ja [ ] Nei | PJL § 22FLK § 6HRL § 21 | [ ] Ja [ ] Nei |
|  | Gjennomfører virksomheten risikovurderinger og vurderer sannsynligheten for og mulige konsekvenser av at en hendelse inntreffer?  | 3.4 | 6.1.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32FLK § 6 | [ ] Ja [ ] Nei |
|  | Gjennomfører virksomheten tiltak for å redusere risikoen dersom risikoen er uakseptabel? | 3.4 | 6.1.38.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32FLK § 7 | [ ] Ja [ ] Nei |
|  | Gjennomføres risikovurdering som minimum før:* etablering av eller endring i behandling av helse- og personopplysninger
* etablering av nye systemer eller registre som inneholder eller benytter helse- og personopplysninger
* det etableres organisatoriske, tekniske eller andre endringer med betydning for informasjonssikkerheten
* det etableres eller endres tilgang til helseopplysninger mellom virksomheter
 | 3.4 | 6.1.2\*8.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 (1)FLK § 6 | [ ] Ja [ ] Nei |
|  | Gjennomfører virksomhetens ledelse jevnlig risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten? | 3.4 | 8.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 24FLK § 8 | [ ] Ja [ ] Nei |
|  | Gjennomføres risikovurdering med utgangspunkt i minimumskravene for konfidensialitet, integritet, tilgjengelighet og robusthet og kontrolleres mot virksomhetens nivå for akseptabel risiko? | 3.4 | 8.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 24 og 32FLK § 8 | [ ] Ja [ ] Nei |
|  | Tas det avgjørende hensyn til konsekvenser for pasient/ bruker og forsvarlig helsehjelp i risikovurderingene? | 3.4 | 6.1.2\* |  |  | [ ] Ja [ ] Nei | HRL § 21 |  |
|  | Dokumenteres risikovurderingene? | 3.4 | 8.2 |  |  | [ ] Ja [ ] Nei | PJL § 23PVF artikkel 5 (2) FLK § 5PVF art. 24 nr. 1 | [ ] Ja [ ] Nei |
|  | Framgår tiltakene, der det er nødvendig å gjennomføre tiltak for å oppnå akseptabel risiko, av en plan der frist og ansvarlig for gjennomføring framgår? | 3.4 | 6.1.3 |  |  | [ ] Ja [ ] Nei | FLK § 5 og 6 | [ ] Ja [ ] Nei |
|  | Er planen for tiltakene forankret hos virksomhetens ledelse? | 3.4 | 5.1 |  |  | [ ] Ja [ ] Nei | FLK § 3 | [ ] Ja [ ] Nei |
|  | Har virksomheten tilstrekkelig kompetanse tilgjengelig for å kunne foreta risikovurderinger? | 3.4 | 7.2 |  |  | [ ] Ja [ ] Nei | FLK § 7 | [ ] Ja [ ] Nei |
|  | Involveres representanter for de som yter helsehjelp i risikovurderinger der det er relevant? | 3.4 | 6.1.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Har de som utfører risikovurderingene en tydelig eskaleringsvei til ledelsen/styret? | 3.4 | 5.3 |  |  | [ ] Ja [ ] Nei | FLK § 8 | [ ] Ja [ ] Nei |
|  | Kommuniseres resultater fra risikovurderingen og plan for oppfølging av tiltak på rett detaljnivå til virksomhetens ledelse og ev. styret der dette er relevant? | 3.4 | 7.4\* |  |  | [ ] Ja [ ] Nei | FL § 9 | [ ] Ja [ ] Nei |
|  | Vurderer virksomheter alltid hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte? | 3.5 | 6.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 (1) |  |
|  | Dokumenterer virksomheten, i en overordnet vurdering, lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoene? | 3.5 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 (1) |  |
|  | Gjennomfører virksomheten en mer grundig personvernkonsekvensvurdering (DPIA) hvis det er sannsynlig at en behandling medfører høy risiko for de registrerte? | 3.5 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 (1) | [ ] Ja [ ] Nei |
|  | Gjennomføres personvernkonsekvensvurderingen før behandlingen av personopplysninger starter? | 3.5.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 (1) |  |
|  | Gjennomføres personvernkonsekvensvurdering når det medfører høy risiko for personvernet?:* når helseopplysninger behandles i stor skala
* ved bruk av ny teknologi
* når personopplysninger behandles på en automatisert, systematisk og omfattende måte, og dette danner grunnlag for avgjørelser som har rettsvirkning eller påvirker den registrerte i betydelig grad
* dersom behandlingens art, omfang, formål og sammenhengen den utføres i, tilsier det

[Konsulter Datatilsynet for liste med når personvernkonsekvensvurdering skal gjennomføres](https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/) | 3.5.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 (1) |  |
|  | Inneholder personvernkonsekvensvurderingen minst?:* en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger
* beskrivelse av formålet med behandlingen av personopplysninger
* vurdering om behandlingene av helse- og personopplysninger er nødvendige og står i rimelig forhold til formålet
* vurdering av risikoene for personvernet til den registrerte
* planlagte risikoreduserende tiltak for ivaretakelse av personvernet
 | 3.5.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 (7) |  |
|  | Blir personvernombudet, om det er utpekt, rådført ved gjennomføring av personvernkonsekvensvurderingen? | 3.5.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 39 (c) | [ ] Ja [ ] Nei |
|  | Blir det planlagt tiltak som reduserer risikoen for personvernet iht. personvernkonsekvensvurderingen? | 3.5.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 35 | [ ] Ja [ ] Nei |
|  | Rådfører den dataansvarlige seg med Datatilsynet, før behandlingen starter, om behandlingen av helse- og personopplysninger vil medføre høy risiko som ikke kan reduseres ved hjelp av rimelige tiltak? | 3.5.1 | A.6.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 36 | [ ] Ja [ ] Nei |
|  | Er behandlingsgrunnlag fastsatt før behandlingen av helse og personopplysningen starter, eller ved endringer i behandlingen? | 4.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 5 nr. 1 bokstav a og 6 |  |
|  | Dekker behandlingsgrunnlaget alle behandlingene som utføres, innsamling, registrering, lagring, sletting, utlevering, mv? | 4.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 6 |  |
|  | Er behandlingsgrunnlaget dokumentert? | 4.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 5 nr. 2  |  |
|  | Har virksomheten lagt til rette for tekniske og organisatoriske tiltak slik at den registrerte kan få innfridd sine rettigheter? | 4.2 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 12, 13, 12, 1524 og 32 |  |
|  | Sørger virksomheten for at alt personell som gis tilgang til helse- og personopplysninger og annen informasjon underlagt taushetsplikt, er kjent med taushetsplikten? | 4.2.1 | A.13.2.4 |  |  | [ ] Ja [ ] Nei | PJL § 15 og 16HPL § 21 og 21 aPVF artikkel 9, 2. i)FLK § 7 | [ ] Ja [ ] Nei |
|  | Legger virksomheten til rette for at personellet kan ivareta taushetsplikten? | 4.2.1 | 5.1\*A.7.2.1\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21 |  |
|  | Behandles brudd på taushetsplikten som avvik? | 4.2.1 | A.7.2.3\*A.16.1\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22FLK § 9PVF artikkel 33 og 34 | [ ] Ja [ ] Nei |
|  | Gir virksomheten informasjon til den registrerte på en kortfattet, åpen, forståelig og lett tilgjengelig måte og med et klart og enkelt språk? | 4.2.2 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 12 |  |
|  | Gis informasjonen til den registrerte skriftlig eller på en annen måte, herunder elektronisk dersom det er hensiktsmessig? | 4.2.2 |  | Pasient-rettigheter |  | [ ] Ja [ ] Nei | PVF artikkel 15 (3)EFF § 3 |  |
|  | Gis den registrerte informasjonen muntlig kun når den registrertes identifiserer seg? | 4.2.2 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 12 |  |
|  | Gir den dataansvarlige, ved innsamling av opplysninger, den registrerte informasjon på en forståelig måte om sine rettigheter og hvordan personopplysningene behandles? | 4.2.2 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 13 og 14 |  |
|  | Sikrer virksomheten at den registrerte kan få innsyn i opplysninger registrert om seg selv? | 4.2.3 |  | Pasient-rettigheter |  | [ ] Ja [ ] Nei | PJL § 18PJF § 11PBL § 5-1PVF artikkel 15 |  |
|  | Sikrer innsynet også loggen over hvem, og eventuelt fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, på hvilket tidspunkt? | 4.2.3 | A.12.4.1\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | PJL § 18, 1. leddPBL § § 5-1, 1.ledd |  |
|  | Sikre virksomheten at den registrerte kan få kunnskap om hvilke personopplysninger om seg selv som virksomheten behandler?Dette omfatter også kunnskap om hvem fra andre virksomheter som har tilegnet seg opplysningene | 4.2.3 | A.8.1.1\* |  |  | [ ] Ja [ ] Nei | PJL § 18PJF § 11PVF artikkel 15 |  |
|  | Sikrer virksomheten at den som gjør sine rettigheter gjeldende er identifisert? | 4.2.3 |  |  |  | [ ] Ja [ ] Nei | PJL § 13 |  |
|  | Gis pasienten, som utgangspunkt innsyn i alle opplysninger i behandlingsrettet helseregister som omhandler seg selv?Dette gjelder også lydopptak, røntgenbilder, videoopptak etc. | 4.2.3.1 |  |  |  | [ ] Ja [ ] Nei | PJL § 18HRL § 24PBL 5-1 |  |
|  | Gir helsepersonell på anmodning forklaring på faguttrykk mv.? | 4.2.3.1 |  |  |  | [ ] Ja [ ] Nei | PBL § 5-1 |  |
|  | Legges det til rette for at samiskspråklige, fremmedspråklige og personer med funksjonshemninger kan utøve innsynsretten? | 4.2.3.1 |  |  |  | [ ] Ja [ ] Nei | PJF § 11 |  |
|  | Dokumenteres det at samiskspråklige, fremmedspråklige og personer med funksjonshemninger kan utøve innsynsretten? | 4.2.3.1 |  |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22 |  |
|  | Nektes pasienten innsyn i opplysninger i journalen eller deler av journalen dersom det er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller innsyn er klart utilrådelig av hensyn til personer som står vedkommende nær? | 4.2.3.1 |  |  |  | [ ] Ja [ ] Nei | PBL § 5-1 |  |
|  | Gir dataansvarlig innsyn innen 30 dager, uten kostnad for pasienten? | 4.2.3.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 12 nr. 3 og 5. |  |
|  | Skjer rettingen i journal ved at oppføringen føres på nytt, eller ved at en datert rettelse tilføyes i journalen?(Retting skal ikke skje ved at opplysninger slettes) | 4.2.4.1 | A.9.1.1\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | HPL § 42 |  |
|  | Utføres retting og sletting som hovedregel av den som har signert opplysningene? | 4.2.4.1 | A.9.1.1\* |  |  | [ ] Ja [ ] Nei | PJF § 15 |  |
|  | Utføres retting eller sletting av helsepersonell utpekt av den dataansvarlige, når den som har signert ikke kan utføre det? | 4.2.4.1 | A.9.1.1\* |  |  | [ ] Ja [ ] Nei | PJF § 15 |  |
|  | Slettes opplysninger som er ført på feil person, med mindre allmenne hensyn tilsier at sletting ikke bør foretas? | 4.2.4.1 | A.9.1.1\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | HPL § 44 |  |
|  | Underretter dataansvarlig enhver mottaker som har fått utlevert personopplysninger som i etterkant er rettet eller slettet(Enhver retting eller sletting av personopplysninger skal meddeles) | 4.2.4.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 17 |  |
|  | Underretter dataansvarlig den registrerte om nevnte mottakere dersom den registrerte anmoder om det? | 4.2.4.1 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 13 og 14 |  |
|  | Orienteres pasienten om klageadgangen dersom krav om retting eller sletting avslås? | 4.2.4.1 |  |  |  | [ ] Ja [ ] Nei | PJF § 15 |  |
|  | Ivaretar virksomheten det overordnede ansvaret for at pasientens rettighet blir ivaretatt?(Opplysninger kan som hovedregel ikke overføres eller tilgjengeliggjøres dersom det er grunn til å tro at pasienten eller brukeren ville motsette seg det dersom den ble spurt. Overføring og tilgjengeliggjøring kan likevel skje dersom tungtveiende grunner taler for det) | 4.2.5.1 |  |  |  | [ ] Ja [ ] Nei | HPL § 25, 1. ledd |  |
|  | Sikrer virksomheten at pasienten gjøres oppmerksom på reservasjonsrettigheten? | 4.2.5.1 |  |  |  | [ ] Ja [ ] Nei | HPL § 10PBL §§ 3-2, 3-3 og 3-4 |  |
|  | Dokumenteres det alltid hvem det er gitt opplysninger til, og hvilken virksomhet denne tilhører? | 4.2.5.1 |  |  |  | [ ] Ja [ ] Nei | PJL § 25 |  |
|  | Gir helsepersonell tilgang til nødvendige og relevante helseopplysninger til samarbeidende personell i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte, med mindre pasienten eller brukeren motsetter seg det? | 4.2.5.2 |  |  |  | [ ] Ja [ ] Nei | HPL § 25 |  |
|  | Er helseopplysningene som utleveres til ledelsen så langt som mulig ikke direkte personidentifiserbare? | 4.2.5.3 | A.8.2\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | HPL § 26, 1. ledd | [ ] Ja [ ] Nei |
|  | Er helseopplysningene som utleveres til ledelsen begrenset til nødvendig og relevant for formålet? | 4.2.5.3 |  |  |  | [ ] Ja [ ] Nei |  |  |
|  | Gir helsepersonell pasientens fødselsnummer og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data til virksomhetsinterne pasientadministrative systemer? | 4.2.5.3 |  |  |  | [ ] Ja [ ] Nei | HPL § 26 |  |
|  | Begrenses helseopplysninger, som tilgjengeliggjøres for læring og kvalitetssikring, til de opplysninger som er nødvendige og relevante for helsepersonellets egen læring eller for kvalitetssikring av helsehjelpen? | 4.2.5.4 | A.8.2\*A.9.1\*A.9.2\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | HPL § 29 c |  |
|  | Dokumenteres det i pasientens journal hvilke opplysninger som er tilgjengeliggjort for læring og kvalitetssikring og hvem de er tilgjengeliggjort til? | 4.2.5.4 |  |  |  | [ ] Ja [ ] Nei | HPL § 29 c |  |
|  | Oppbevares helseopplysninger til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem? | 4.2.6.1 | A.8.1\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | PJL § 25 | [ ] Ja [ ] Nei |
|  | Oppbevares opplysninger om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logger) til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem? | 4.2.6.1 | A.8.1\* | Logging |  | [ ] Ja [ ] Nei | PJL § 25 | [ ] Ja [ ] Nei |
|  | Blir opplysningene slettet hvis de deretter ikke skal bevares etter arkivloven, helsearkivloven eller annen lovgivning? | 4.2.6.1 | A.8.1.2\* | Pasient-rettigheter |  | [ ] Ja [ ] Nei | PJL § 25 |  |
|  | Gjenspeiler elektronisk behandlingsrettet helseregister alltid originalen etter digitalisering? | 4.2.6.2 | A.8.1.3\* |  |  | [ ] Ja [ ] Nei | PJF § 16 |  |
|  | Tar virksomheten og leverandører hensyn til personvern i alle utviklingsfaser av et system eller en løsning? | 4.3 | A.14.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32 |  |
|  | Sørger virksomheten for at informasjonssystemene oppfyller personvernprinsippene og at de ivaretar de registrertes rettigheter? | 4.3 | A.14.1\*A.14.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 25 |  |
|  | Velger dataansvarlig leverandører som er i stand til å levere tjenester som oppfyller lovbestemte krav og krav i Normen? | 4.3 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 nr. 1 |  |
|  | Bidrar leverandører til at dataansvarlig, som tar i bruk leverandørens produkter og tjenester, kan oppfylle kravene?Om nødvendig må partene gå i dialog for å finne riktige tiltak for å kunne oppfylle kravene. | 4.3 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Er sikkerhetstiltak egnede og valgt på grunnlag av risikovurderinger? | 5 | 6.1.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Vurderer virksomheten om det er nødvendig å gjennomføre mer omfattende tiltak enn det som er beskrevet i kapittel 5 i Normen? | 5 | 6.1.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 8 | [ ] Ja [ ] Nei |
|  | Læres alle medarbeidere i virksomheten kontinuerlig opp i krav som gjelder ivaretakelse av taushetsplikten, informasjonssikkerheten og personvernet? | 5.1.1 | 7.2\*7.3\*A.7.2.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 7 | [ ] Ja [ ] Nei |
|  | Innhenter virksomheten taushetserklæring for den enkelte medarbeider? | 5.1.1 | A.7.1.2A.13.2.4 |  |  | [ ] Ja [ ] Nei | PJL § 15, 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Har virksomheten retningslinjer for privat bruk av informasjonssystemer og utstyr? | 5.1.1 | A.8.1.3 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22FLK § 7 | [ ] Ja [ ] Nei |
|  | Har virksomheten etablert tiltak som ivaretar at alle som gis tilgang til informasjonssystemer og tilhørende informasjon, har tilstrekkelig kompetanse til å benytte systemene og til å ivareta informasjonssikkerheten og personvernet til den registrerte? | 5.1.2 | A.7.2.1A.7.2.2 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23HRL §§ 21 og 22FLK § 7 | [ ] Ja [ ] Nei |
|  | Er kompetansebyggingen kontinuerlig og tilpasset ulike roller og brukergrupper? | 5.1.2 | A.7.2.2 |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23HRL §§ 21 og 22FLK § 7 | [ ] Ja [ ] Nei |
|  | Vurderes nye opplæringstiltak ved teknologiske endringer eller endring i rutiner? | 5.1.2 | (A.7.2.2\*&A.12.1.2\*) |  |  | [ ] Ja [ ] Nei | PJL §§ 22 og 23HRL § 21 og 22FLK § 7 | [ ] Ja [ ] Nei |
|  | Leveres alle medier (herunder digitalt, papir, osv.) som kan inneholde helse- og personopplysninger når et arbeidsforhold opphører? | 5.1.3 | A.8.1.4 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Leveres adgangskort tilbake og deaktiveres ved opphør i arbeidsforhold? | 5.1.3 | (A.8.1.4\*,A.9.2.6\*&A.11.1.2\*) |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Sperres all tilgang ved opphør i arbeidsforhold? | 5.1.3 | A.9.2.6 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Har virksomheten rutiner for å rydde opp i informasjon den ansatte kan ha lagret på egen brukerkonto? | 5.1.3 | A.8.1.4\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22FLK § 7 | [ ] Ja [ ] Nei |
|  | Har virksomheten rutiner for autorisering, endring og avslutning av tilganger? | 5.2 | A.9.2.1A.9.2.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21PJF § 13 | [ ] Ja [ ] Nei |
|  | Sørger virksomheten for, innenfor rammen av taushetsplikten, at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte? | 5.2 | A.9.2\* |  |  | [ ] Ja [ ] Nei | PJL §§ 15,19HPL §§ 21, 25PVF artikkel 32 nr. 1 bokstav b | [ ] Ja [ ] Nei |
|  | Sørger virksomheten for at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten og personvernet? | 5.2 | A.9.1.1\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er tilgangsstyring etablert for alle informasjonssystemer? | 5.2 | A.9.1  | Autorisering |  | [ ] Ja [ ] Nei | PJL § 22PJF § 13HFL § 7, 1. leddHPL §25, 2.leddPVF artikkel 32 nr. 1 bokstav b | [ ] Ja [ ] Nei |
|  | Er tilgangsstyring etablert for administrator- og systembrukere? | 5.2 | A.9.2.3 | Autorisering |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Sikres det at bare autorisert personell med tjenstlige behov får tilgang til helse- og personopplysninger? | 5.2 | A.9.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Gis tilgang til behandlingsrettede helseregistre etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten?  | 5.2 | A.8.1.3\* | Autorisering |  | [ ] Ja [ ] Nei | PJL § 19 |  |
|  | Styres tilgang slik at taushetspliktreglene ivaretas og at tilgang til helse- og personopplysninger ikke gis til andre enn dem som har tjenstlig behov? | 5.2 | A.9.2\*A.9.4\* |  |  | [ ] Ja [ ] Nei | PJL §§ 19, 22HPL § 25PJF § 13, 1. ledd, a) | [ ] Ja [ ] Nei |
|  | Vurderes og ivaretas lovbestemt taushetsplikt ved tildeling av autorisasjon? | 5.2.1 | A.9.2.1\*A.9.4.1\* |  |  | [ ] Ja [ ] Nei | PJL §§ 15, 23PJF §§ 13, 1. ledd, a), 15 | [ ] Ja [ ] Nei |
|  | Sikrer tildelt autorisasjon at den enkelte kan få tilgang til relevante og nødvendige helse- og personopplysninger i samsvar med personellets ansvar og oppgaver, så langt lovbestemt taushetsplikt ikke er til hinder for det? | 5.2.1 | A.9.2\* | Autorisering |  | [ ] Ja [ ] Nei | PJL §§ 19, 22PJF § 13, 1. ledd | [ ] Ja [ ] Nei |
|  | Vurderes autorisasjonen på nytt når det oppstår endringer i ansvarsområder eller ansettelsesforhold eller langvarig fravær? | 5.2.1 | A.9.2.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Benyttes det roller i virksomheten skal autorisering for hver rolle skje uavhengig av personellets øvrige roller? | 5.2.1 | A.9.1\*A.9.2\* | Autorisering |  | [ ] Ja [ ] Nei | PJL § 13 | [ ] Ja [ ] Nei |
|  | Er autorisasjonen for tilgang til behandlingsrettede helseregister tidsbegrenset? | 5.2.1 | A.9.2.2\* | Autorisering |  | [ ] Ja [ ] Nei | PJF § 13 | [ ] Ja [ ] Nei |
|  | Angir autorisasjonen for tilgang til behandlingsrettede helseregister hvilke virksomheter autorisasjonen omfatter? | 5.2.1 | A.9.1\*A.9.2\* | Autorisering |  | [ ] Ja [ ] Nei | PJF § 13 | [ ] Ja [ ] Nei |
|  | Er det etablert tiltak slik at mulig misbruk av autorisert teknisk personell, med særskilt behov for tilgang til større mengder helse- og personopplysninger, skal kunne avdekkes? | 5.2.1 | A.12.4.3 |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21FLK § 7 | [ ] Ja [ ] Nei |
|  | Grunngis og registreres bruk av selvautorisering? | 5.2.1 | A.12.4\*A.16.1\* | Autorisering |  | [ ] Ja [ ] Nei | PJL § 19, 2. ledd | [ ] Ja [ ] Nei |
|  | Er det etablert tekniske tiltak slik at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i informasjonssystemene hvem som har endret og hva som er endret?Eksempler på sikkerhetskrav der det ikke benyttes PKI: Passordfil skal krypteres | 5.2.1 | A.12.4.1 | Autentisering |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Registreres all tildeling av autorisasjon i et autorisasjonsregister? | 5.2.1 | A.9.2.1\* | Autorisasjon |  | [ ] Ja [ ] Nei | PJF 13, 1.ledd, c) | [ ] Ja [ ] Nei |
|  | Er det etablert tekniske tiltak for å sikre at personer i eller utenfor virksomheten ikke skal kunne endre konfigurasjon og programvare uten at det logges? | 5.2.1 | A.12.4.3 | Logging |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Benytter bruker med administratortilganger personlig separat brukerkonto for administratoroppgaver? | 5.2.1 | A.9.2.3 | Autorisering |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Har driftspersonell personlige brukerkonto for oppgaver som ikke krever administratortilganger? | 5.2.1 | A.9.2.3 | Autorisering |  |  | PVF artikkel 32PJL § 22HRL § 21 |  |
|  | Er det etablert ulike administratorbrukere til de ulike delene av infrastrukturen som forvaltes? | 5.2.1 | A.9.2.3 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er det gjennomført risikovurdering som begrunner behovet for ulike administratorbrukere? | 5.2.1 | (8.2\*&A.9.2.3\*) |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Har virksomheten sørget for at det opprettes et autorisasjonsregister som minimum inneholde:* informasjon om hvem som er tildelt autorisasjon
* til hvilken rolle autorisasjonen er tildelt (om rolle benyttes i virksomheten)
* formålet med autorisasjonen
* tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt
* informasjon om hvilken virksomhet den autoriserte er knyttet til
* helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk)

Eksempler på sikkerhetskrav: Det skal også registreres hvem (fysisk identifiserbar person) som har opprettet (registrert) autorisasjonen | 5.2.1.1 | A.9.2.1\* | Autorisering |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PJF § 13, 1.ledd c) | [ ] Ja [ ] Nei |
|  | Har virksomheten kontroll og oversikt over all behandling av helse- og personopplysninger som den er ansvarlig for? | 5.2.1.2 | A.8.1.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 55 |  |
|  | Har virksomheten oversikt over tilgjengeliggjøring av opplysninger til andre virksomheter? | 5.2.1.2 | A.8.1.1\*A.13.2.2\* | Logging |  | [ ] Ja [ ] Nei | PJF § 13, 1. ledd b) | [ ] Ja [ ] Nei |
|  | Er det gjennomført risikovurdering ved oppstart eller endring av tilgjengeliggjøring av opplysninger for andre virksomheter? | 5.2.1.2 | 8.2\* |  |  | [ ] Ja [ ] Nei | PJL § 19, 2. ledd | [ ] Ja [ ] Nei |
|  | Har dataansvarlig og virksomhetene som gis tilgang til opplysninger hos dataansvarlig avklart gjennom avtale eller på annen måte:* hvordan autentisering skal foregå på en sikker måte
* hvordan autorisering til helseopplysninger hos dataansvarlig skal foregå
* hvordan logging og oppfølging av logger skal foregå
 | 5.2.1.2 | A.13.2.2\*A.9.1\*A.9.2\*A.12.4\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21 |  |
|  | Bekrefter den autoriserte sin identitet på en sikker måte? | 5.2.2 | A.9.4.2 | Autentisering |  | [ ] Ja [ ] Nei | PJF § 13, 2. ledd | [ ] Ja [ ] Nei |
|  | Besluttes sikker måte på grunnlag av en risikovurdering? | 5.2.2 | 8.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Identifiseres ulike ansettelsesforhold ved autentisering?  | 5.2.2 | A.9.1 | Autentisering |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Sikres det at flere personer ikke benytter samme autentiseringskriteria?Eksempler på sikkerhetskrav der det ikke benyttes PKI: * Passordet skal kunne byttes enkelt av bruker
* Tvunget skifte av passord skal være teknisk mulig
* Passordets kvalitet og varighet skal kunne konfigureres
 | 5.2.2 | A.9.4 | Autentisering |  | [ ] Ja [ ] Nei | PJF § 13, 2. ledd | [ ] Ja [ ] Nei |
|  | Tildeles autentiseringskriteria (som brukernavn og passord) på en betryggende måte? | 5.2.2 | (A.9.2.2\*,A.9.2.3\*&A.9.2.4\*) |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PJF § 13, 2. ledd | [ ] Ja [ ] Nei |
|  | Sikres tilgang fra hjemmekontor og/eller mobilt utstyr (og mobilnettverk) ved sikker autentiseringsløsning? | 5.2.2 | (A.6.2.2\*&A.9.4.2\*) |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PJF § 13, 2. ledd | [ ] Ja [ ] Nei |
|  | Er alle standardpassord (fabrikkinnstillinger) på systemer og utstyr endret før behandling av helse- og personopplysninger starter? | 5.2.2 | A.9.4.3\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Autentiseres den autoriserte brukeren med sikker autentiseringsløsning ved bruk av trådløse nettverk for behandling av helse- og personopplysninger? | 5.2.2 | (A.9.1.2\*&A.9.4.2\*) | Autentisering |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PJF § 13, 2. ledd | [ ] Ja [ ] Nei |
|  | Identifiseres den enkelte rolle om roller benyttes?  | 5.2.2 | A.9.1.1\* | Autentisering |  | [ ] Ja [ ] Nei |  | [ ] Ja [ ] Nei |
|  | Gis det ved behov ny autentisering ved bytte av rolle (om roller benyttes)? | 5.2.2 | A.9.4.2\* | Autentisering |  | [ ] Ja [ ] Nei |  | [ ] Ja [ ] Nei |
|  | Påser virksomhetens ledelse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang?Eksempler på sikkerhetskrav: Behandlingsrettet helseregister må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt. | 5.2.3 | A.9.2.5 | Autorisering |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21PJF § 13, 1. ledd bokstav e) og 3. leddPVF art. 5 nr. 1 bokstav f | [ ] Ja [ ] Nei |
|  | Foretar den enkelte leder gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner:* Ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde?
* Minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)?
* Ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet?
 | 5.2.3 | (A.9.2\*,A.12.1.2\*&A.17.1.3\*) |  |  | [ ] Ja [ ] Nei | PJL § 22 og 23HRL §§ 21 og 22PJF § 13, 1. ledd bokstav e) og 3. ledd | [ ] Ja [ ] Nei |
|  | Varles virksomhetens ledelse dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang? | 5.2.3 | A.16.1.5 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Dersom kontrollen viser at det har skjedd en urettmessig tilgang, behandles det som et avvik,? | 5.2.3 | A.16.1.4 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 33 | [ ] Ja [ ] Nei |
|  | Følges misbruk av selvautorisering opp som avvik? | 5.2.3 | A.12.4\*A.16.1\*A.7.2.3\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Samarbeider avtalepartene, ved bruk av tilgang til helseopplysninger mellom virksomheter, om kontroll av tilganger? | 5.2.3 | A.13.2.2\*A.15.1\*A.15.2\*A.9.2.5\* |  |  | [ ] Ja [ ] Nei | PJL § 9, 1. ledd c) | [ ] Ja [ ] Nei |
|  | Kontrollerer den dataansvarlige, som har adgang til å autorisere helsepersonell for tilgang mellom virksomheter, løpende:* hvem i egen virksomhet som elektronisk har hentet frem helseopplysninger fra annen virksomhet
* hvorfor dette er gjort
* tidsperioden helseopplysningene er hentet frem
 | 5.2.3 | A.13.2.2\*A.15.2\*A.12.4.1\*A.16.1\* | Autorisering |  | [ ] Ja [ ] Nei | PJL § 14 | [ ] Ja [ ] Nei |
|  | Varsles virksomheten opplysningene er hentet fra, om kontrollen viser at noen urettmessig har hentet frem helseopplysninger? | 5.2.3 | A.13.2.2\*A.16.1\* |  |  | [ ] Ja [ ] Nei | PJF § 14, 3. ledd | [ ] Ja [ ] Nei |
|  | Varsles pasienten/brukeren, av virksomheten opplysningene er hentet fra, om kontrollen viser at noen urettmessig har hentet frem helseopplysninger? | 5.2.3 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 34 |  |
|  | Behandles avviket (om urettmessig fremhenting av helseopplysninger) iht. etablerte prosedyrer for avviksbehandling? | 5.2.3 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 33 | [ ] Ja [ ] Nei |
|  | Er det etablert rutine for administrasjon av nøkler/adgangskort i adgangskontrollsystemet? | 5.3.1 | A.11.1.2 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Er det etablert sikkerhetstiltak som hindrer at uautoriserte får tilgang til helse- og personopplysninger?Dette kan løses ved adgangskontroll av lokaler med utstyr og ved at IKT-utstyret sikres mot misbruk eller uautorisert innsyn. | 5.3.2 | A.11.1 |  |  | [ ] Ja [ ] Nei | PJL §§ 22, 23HRL §§ 21 og 22PVF artikkel 32PVF art. 5 nr. 1 bokstav f | [ ] Ja [ ] Nei |
|  | Er det etablert sikkerhetstiltak som hindrer at annet enn autorisert personell får adgang til infrastruktur? | 5.3.3 | A.11.1 |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Slettes alle lagringsmedia forsvarlig når de tas ut av bruk?Plikt til arkivering av opplysningene skal uansett overholdes. | 5.3.3 | (A.8.3.2\*&A.11.2.7\*) |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 17 og 32 | [ ] Ja [ ] Nei |
|  | Gjennomføres det risikovurdering av løsningene som benyttes for mobilt utstyr og hjemmekontor før løsningene tas i bruk og ved endringer som kan påvirke informasjonssikkerheten? | 5.3.4 | A.11.2.6\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er det etablert administrative rutiner for bruk av mobilt utstyr og hjemmekontor? | 5.3.4 | A.6.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Lagres helse- og personopplysninger lokalt bare når dette er nødvendig ut fra tjenstlig behov og kryptert? | 5.3.4 | A.8.1.3\*A.8.2.3\*A.10.1.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er det iverksatt tekniske tiltak slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres? | 5.3.5 | A.10.1\*A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Blir kryptering og dekryptering, mellom kommunikasjonspunkter i infrastrukturen, gjort i godkjent utstyr virksomheten har kontroll med?Kontrollen kan ivaretas gjennom avtale. | 5.3.5 | A.10.1\*A.13.1.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Krypteres all kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer? | 5.3.5 | (A.10.1\*&A.13.2\*) |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Krypteres lagrede direkte identifiserbare personopplysninger som behandles iht. helseregisterloven §§ 10 og 11? | 5.3.5 | A.8.1.3\*A.8.2.3\*A.10.1.1\* |  |  | [ ] Ja [ ] Nei | HRL § 21PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Inkluderes medisinsk utstyr som behandler helse- og personopplysninger i virksomhetens arbeid med informasjonssikkerhet, herunder i risikovurderinger, tilgangsstyring, endringskontroll og rutiner for bruk, på linje med andre informasjonssystemer? | 5.3.6 | (A.11.2\*,A.14.1.1\*,A.9.4\*,A.14.2.2\*&A.8.1.3\*) |  |  | [ ] Ja [ ] Nei | PJL § 22PVF artikkel 32Håndteringsforskriften § 11? | [ ] Ja [ ] Nei |
|  | Sikrer konfigurasjonen at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt? | 5.4.1 | (A.12.5.1\*&A.14.2.2\*) |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21PVF art. 25 | [ ] Ja [ ] Nei |
|  | Sørger virksomheten for at all dataflyt, datakommunikasjon og integrasjoner kartlegges og dokumenteres? | 5.4.1 | A.12.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 5 nr. 2 og 32PJL § 22HRL § 21FLK § 7 og 5 | [ ] Ja [ ] Nei |
|  | Sikres det at kun godkjent utstyr og programvare benyttes til behandling av helse- og personopplysninger? | 5.4.1 | A.12.6.2\*A.8.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21EFF § 17 | [ ] Ja [ ] Nei |
|  | Har virksomheten fastsatt hvem som godkjenner utstyr og programvare som benyttes til behandling av helse- og personopplysninger? | 5.4.1 | A.12.5.1\*A.6.1.1\*A.8.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 7 | [ ] Ja [ ] Nei |
|  | Oppdateres maskin- og programvare slik at den nyeste og mest tidsaktuelle sikkerhetsfunksjonaliteten følger med og nødvendige sikringstiltak benyttes? | 5.4.1 | A.12.6 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 15 | [ ] Ja [ ] Nei |
|  | Gjennomføres planlagte endringer iht virksomhetens rutine for konfigurasjonsendringer? | 5.4.1 | A.14.2.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 17EFF § 15 | [ ] Ja [ ] Nei |
|  | Benyttes det separate miljøer for utvikling, test og produksjon slik at helse- og personopplysninger som benyttes ved ytelse av helsehjelp, ikke blir påvirket ved feil i utvikling og test? | 5.4.1 | A.12.1.4 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Sjekkes konfigurasjonen av utstyr og programvare jevnlig slik at den kun utfører formålsbestemte funksjoner? | 5.4.1 | (A.12.1.1\*&A.12.5.1\*) |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 7EFF § 15PVF art. 25 | [ ] Ja [ ] Nei |
|  | Er konfigurasjonen beskyttet mot ondsinnet programvare? | 5.4.1 | A.12.2.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er konfigurasjonen beskyttet mot utilsiktede handlinger? | 5.4.1 | A.14.2.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF Artikkel 32 | [ ] Ja [ ] Nei |
|  | Blir konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, først satt i drift når:* Risikovurdering som viser at nivå for akseptabel risiko oppfylles?
* Test som sikrer at forventede funksjoner er ivaretatt?
* Implementering som sikrer mot uforutsette hendelser?
* Ny konfigurasjon er dokumentert?
* Konfigurasjonsendringer er godkjent av virksomhetens leder eller den ledelsen bemyndiger?
 | 5.4.1 | A.14.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 5 og 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Er konfigurasjonskontroll regulert gjennom avtale ved:* Bruk av databehandler?
* Bruk av fjernaksess for vedlikehold og oppdateringer (Fjernaksess skal kun gjøres over kanaler virksomheten har kontroll med.)?
 | 5.4.1 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Blir alle endringer med betydning for informasjonssikkerheten i organisasjonen, informasjonssystemene og infrastruktur forankret på relevant ledernivå? | 5.4.1 | (A.12.1.2\* &5.1\*) |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22FKL § 3 og 7 | [ ] Ja [ ] Nei |
|  | Har virksomheten utarbeidet rutiner for endringsledelse som omfatter følgende temaer:* Identifisering av vesentlige endringer
* Planlegging og testing av endringer
* Vurdering av potensielle konsekvenser, for eksempel ved å gjennomføre en risikovurdering og eventuelt en personvernkonsekvensvurdering
* Godkjennelsesprosedyre for endringer?
* Kommunikasjon av plan til aktuelle personer/roller
* Reserverutiner om endringen må avbrytes, feiler eller at uønskede hendelser oppstår
* Endringslogg med relevante opplysninger
* Opplæring av berørte brukere/roller
 | 5.4.2 | A 12.1.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32, 35PJL § 23HRL § 22FKL § 6, 7 | [ ] Ja [ ] Nei |
|  | Sørger virksomhetens ledelse for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal drift? | 5.4.3 | A.12.3.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Oppbevares sikkerhetskopier avlåst og brannsikret, og adskilt fra driftsutstyret? | 5.4.3 | A.12.3.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 7 | [ ] Ja [ ] Nei |
|  | Testes det jevnlig at sikkerhetskopiene er korrekte og kan tilbakeføres? | 5.4.3 | A.12.3.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FKL § 7 og 8 | [ ] Ja [ ] Nei |
|  | Er minimum en sikkerhetskopi beskyttet mot ondsinnet programvare og uønskede hendelser? | 5.4.3 | A.12.3.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Logges det som minimum:* Autorisert bruk av informasjonssystemene
* All system- og administratorbruk til informasjonssystemer og infrastrukturen
* Endring av konfigurasjon og programvare
* Sikkerhetsrelevante hendelser i sikkerhetsbarrierer
* Forsøk på uautorisert bruk av informasjonssystemer og infrastrukturen
* Bruk av selvautorisering
 | 5.4.4 | A.12.4\* | Logging |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32PJF § 14 | [ ] Ja [ ] Nei |
|  | Registreres som minimum følgende i loggene ved autorisert bruk av behandlingsrettet helseregister:* Identitet til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger
* Organisatorisk tilhørighet
* Grunnlaget for tilgjengeliggjøringen
* Tidsperioden for tilgjengeliggjøringen
 | 5.4.4 | A.12.4.1\* | Logging |  | [ ] Ja [ ] Nei | PJF § 14, 1. leddHPL § 45, 1. ledd | [ ] Ja [ ] Nei |
|  | Besluttes kravene til logging, ved behandling av helse- og personopplysninger for andre formål enn ytelse av helse- og omsorgstjenester, på grunnlag av en risikovurdering? | 5.4.4 | 8.2\*A.12.4.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 7 | [ ] Ja [ ] Nei |
|  | Kan loggene enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd? | 5.4.4 | A.12.4.1\* |  |  | [ ] Ja [ ] Nei | PJF § 14, 3. ledd | [ ] Ja [ ] Nei |
|  | Er det etablert rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser? | 5.4.4 | A.12.4.1\*A.12.4.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Håndteres det som et avvik om brudd avdekkes ved analyse av loggene? | 5.4.4 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PJL § 14PVF artikkel 33 og 34 | [ ] Ja [ ] Nei |
|  | Et det etablert rutiner for ved behov å kunne sammenholde loggene med autorisasjonsregister? | 5.4.4 | A.12.4.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 23HRL § 22PJF § 13  | [ ] Ja [ ] Nei |
|  | Sikres logger og autorisasjonsregister mot endring og sletting? | 5.4.4 | A.12.4.2A.12.4.3 | Logging |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22 og 42HRL § 21PJF § 13 og 15PVF art. 5 nr. 1 bokstav f | [ ] Ja [ ] Nei |
|  | Har logger korrekt tidsstempel? | 5.4.4 | A.12.4.1A.12.4.4 | Logging |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21PJF § 14 | [ ] Ja [ ] Nei |
|  | Lagres logger, som genereres ved ytelse av helsehjelp, til det ikke antas å være bruk for dem? | 5.4.4 | 12.4.2\* | Logging |  | [ ] Ja [ ] Nei | PJL § 25 | [ ] Ja [ ] Nei |
|  | Følger styring og håndtering av tekniske sårbarheter rutinene for endringsstyring? | 5.4.5 | (A.12.6.1\* & A.12.1.2\*) |  |  | [ ] Ja [ ] Nei | PJL § 23, 1. leddFLK § 7 | [ ] Ja [ ] Nei |
|  | Har virksomheten rutiner for å skaffe seg informasjon om tekniske sårbarheter i utstyr og programvare? | 5.4.5 | A.12.6.1 |  |  | [ ] Ja [ ] Nei | PJL § 23, 1. leddFLK § 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Er det etablert rutiner og operative tiltak som ivaretar:* Ansvaret for: overvåkning, risikovurdering, korrigering og koordinering
* Hvordan virksomheten skal reagere og varsle om sårbarheter
* Prioritering og etablering av tidslinje for korrigering
 | 5.4.5 | (A.12.6.1\*,A.12.1.2\*&A.16.1.5\*) |  |  | [ ] Ja [ ] Nei | PVF art. 32PJL § 23, 1. leddFLK § 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Følger virksomhetens ledelse opp at sikkerheten ivaretas ved jevnlige og minimum årlige sikkerhetsrevisjoner? | 5.4.6 | 9.2\* |  |  | [ ] Ja [ ] Nei | PJL § 23, 1. leddPVF artikkel 32 (1)(d)FKL § 8 | [ ] Ja [ ] Nei |
|  | Foreligger det en godkjent plan for sikkerhetsrevisjoner? | 5.4.6 | 9.2 |  |  | [ ] Ja [ ] Nei | PJL § 23, 1. leddPVF artikkel 32 (1)(d)FKL § 6 | [ ] Ja [ ] Nei |
|  | Dokumenteres og håndteres resultatene, konklusjonene og avvikene fra sikkerhetsrevisjonene av virksomheten? | 5.4.6 | (9.2\* & 10.1\*) |  |  | [ ] Ja [ ] Nei | PJL § 23, 2. leddFKL § 5 og 8 | [ ] Ja [ ] Nei |
|  | Har virksomheten tydelig definert hvilke krav som gjelder for nettverkssikkerhet, og er tiltakene som er iverksatt basert på en risikovurdering? | 5.5.1 | (A.13.1\* & 6.1.2\*) |  |  | [ ] Ja [ ] Nei | PJL § 22, 1. leddHRL § 21PVF artikkel 32, 1. b) og 35FLK § 6 og 7 | [ ] Ja [ ] Nei |
|  | Er det etablert tekniske tiltak ved tilkobling til eksterne nett utenfor virksomheten som ivaretar at:* Kun eksplisitt angitt tillatt trafikk kan passere utenfra og inn eller motsatt, annet stoppes
* I tiltaket skal det være minst to uavhengige, tekniske tiltak slik at personer utenfor virksomheten ikke skal kunne få uautorisert tilgang til og/eller kunne endre eller slette helse- og personopplysninger
 | 5.5.2 | A.13.1\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32, 1. b)FLK § 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Er det etablert klare ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler ved meldingsformidling? | 5.5.3.1 | A.13.2 |  |  | [ ] Ja [ ] Nei | FLK § 3, 7 og 8 | [ ] Ja [ ] Nei |
|  | Er alle avtaler for meldingsformidling skriftlige? | 5.5.3.1 | A.13.2.2 |  |  | [ ] Ja [ ] Nei |  | [ ] Ja [ ] Nei |
|  | Er det avtalt at avsender/tilbyende virksomhet er ansvarlig for* egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging
* at tjenesten ikke skal kunne formidle program som inneholder ondsinnet programvare e.l.
* sikker overføringskryptering ende-til-ende
 | 5.5.3.1 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er det avtalt at mottaker/anvendende virksomhet er ansvarlig for:* å sikre at tjenesten ikke skal kunne formidle ondsinnet kode el.
* egen tilkoblingssikring som hindrer utilsiktet tilgjengeliggjøring og inntrenging
* å ivareta overføringskryptering ende-til-ende
 | 5.5.3.1 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Er det ved meldingskommunikasjon basert på ebXML rammeverket avtalt at avsender er ansvarlig for* rett adressering av elektroniske samhandlingsmeldinger i.h.t. adresseregisteret
* at meldingen ved behov skal være signert på en slik måte at virksomheten ikke kan benekte å ha sendt den
* avviksrapportering i forbindelse med feilsending
* at melding skal avleveres i avtalt format
 | 5.5.3.2 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21EFF § 27 | [ ] Ja [ ] Nei |
|  | Er det ved meldingskommunikasjon basert på ebXML rammeverket avtalt at mottaker er ansvarlig for* å registrere mottaket ved behov slik at mottaker ikke kan benekte å ha mottatt meldingen
* avviksrapportering i forbindelse med feil, dvs. mottak av melding som ikke er adressert til virksomheten
* at melding skal mottas i avtalt format
 | 5.5.3.2 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21EFF § 27 | [ ] Ja [ ] Nei |
|  | Er det ved meldingskommunikasjon basert på ebXML rammeverket avtalt at meldingsformilder er ansvarlig for* at melding kun skal avleveres til adressaten
* at melding ikke skal endres eller destrueres under transport fra avsender til mottaker
* at melding ikke skal kunne leses av andre enn avsender og mottaker
* at melding skal avleveres innen avtalte tidsfrister fra avsendelse
* avviksrapportering i forbindelse med alle ovenstående punkter
 | 5.5.3.2 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 7 | [ ] Ja [ ] Nei |
|  | Ivaretas følgende sikkerhetsprinsipper ved datadeling* Det må være en sikker brukerautentisering som virksomhetene som tilbyr datadelingsgrensesnitt har tillit til
* Virksomheten som ber om tilgang skal kontrollere at brukeren har nødvendige autorisasjoner for det aktuelle datadelingsgrensesnittet
* Det skal skilles mellom lese- og skriverettigheter til forskjellige informasjonselementer basert på den enkelte brukerautorisasjon
* Unødvendig mellomlagring skal unngås
* Det skal være mulig å kunne verifisere legitimiteten til datadelingsgrensesnittet og virksomheten som tilbyr den
* Felleskomponenter for autentisering av konsument skal benyttes der det er tilgjengelig og hensiktsmessig
 | 5.5.3.3 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21FLK § 7EFF § 15 | [ ] Ja [ ] Nei |
|  | Har virksomheten etablert tiltak for å forhindre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten tilgjengeliggjøres ved hjelp av ukryptert e-post og SMS eller andre usikre kanaler? | 5.5.4 | A.13.2.1 |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32, 1. b)FLK § 7EFF § 7 og 15PVF art. 5 nr. 1 bokstav f | [ ] Ja [ ] Nei |
|  | Forsikrer virksomheten seg med tekniske tiltak og organisatoriske tiltak, når det brukes ukrypterte kanaler, at e-post ikke inneholder identifiserbare helseopplysninger? | 5.5.4 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32, 1. b)EFF § 7 og 15 | [ ] Ja [ ] Nei |
|  | Iverksetter virksomheten logging, når det brukes ukrypterte kanaler, for å kontrollere at regler ikke brytes? | 5.5.4 | A.13.2\*A.12.4\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32, 1. b)EFF § 7 og 15 | [ ] Ja [ ] Nei |
|  | Håndterer virksomheten regelbrudd, når det brukes ukrypterte kanaler, som avvik og vurderes personalmessige konsekvenser? | 5.5.4 | (A.10.1.1\*,A.16.1\* &A.7.2.3\*) |  |  | [ ] Ja [ ] Nei | PJL § 23, 1. leddHRL § 22EFF § 7 og 15FLK § 8 | [ ] Ja [ ] Nei |
|  | Vurderer virksomheten, når det brukes ukrypterte kanaler, om den samlede informasjonen i SMS og e-post kan medføre brudd på taushetsplikten | 5.5.4 | A.8.1.3\*A.8.2.3\* |  |  | [ ] Ja [ ] Nei | PJL § 15HPL § 21PVF artikkel 9, 2. i)EFF § 7 og 15 | [ ] Ja [ ] Nei |
|  | Er alt teknisk utstyr eller applikasjoner som kobles til Internett inkludert i virksomhetens arbeid med informasjonssikkerhet og personvern, herunder i risikovurderinger, tilgangsstyring og rutiner for bruk? | 5.5.5 | A.14.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32, 1. b)FLK § 6, 7 og 8 | [ ] Ja [ ] Nei |
|  | Har virksomheten iverksatt følgende tiltak ved tilkobling til Internett: * tekniske tiltak som bidrar til å hindre utilsiktet utlevering og uautorisert tilgang til helse- og personopplysninger?
* logging for å kontrollere at regler ikke brytes og at regelbrudd skal håndteres som avvik?
 | 5.5.5 | A.14.1.2\*A.15.1.3\*A.7.2.3\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32, 1. b)EFF § 15FLK § 7 | [ ] Ja [ ] Nei |
|  | Vurderer og beslutter virksomheten behandlingsgrunnlaget ved digital kommunikasjon med den registrerte? | 5.6 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 6 og 9 |  |
|  | Vurdere virksomheten egnet løsning og kommunikasjonskanal ved digital kommunikasjon med den registrerte? | 5.6 | A.13.2\*A.8.1.3\*A.8.2.3\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32EFF § 3 | [ ] Ja [ ] Nei |
|  | Sørger virksomheten for at helse- og personopplysninger ikke stilles til rådighet på en slik måte at pasient/bruker er avhengig av å lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen? | 5.6 | A.13.2\*A.8.1.3\*A.8.2.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 25 | [ ] Ja [ ] Nei |
|  | Sørger virksomheten for at det er etablert rutiner som ivaretar at meldingen til pasienten ikke er inngripende og krenker personvernet, men samtidig har tilstrekkelig informasjon til pasienten? | 5.6 | A.8.1.3\*A.8.2.3\*8.2\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22EFF § 8 |  |
|  | Gjennomfører virksomheten tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker? | 5.6 | A.9.4.2\*A.13.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32EFF § 8PVF art. 5 nr. 1 bokstav f | [ ] Ja [ ] Nei |
|  | Tilrettelegger leverandøren for at dataansvarlig, som tar i bruk leverandørens produkter og tjenester, kan oppfylle lovbestemte krav og krav i Normen? | 5.7 | A.15.1.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 28FLK § 7 | [ ] Ja [ ] Nei |
|  | Forsikrer leverandøren at de har rutiner som pålegger alle medarbeidere taushetsplikt om helse- og personopplysninger og annen taushetsbelagt informasjon? | 5.7.1 | (A.15.1.2\*&A.13.2.4\*) |  |  | [ ] Ja [ ] Nei | PJL § 15HPL § 21PVF art. 5 nr. 1 bokstav fPVF art 32 | [ ] Ja [ ] Nei |
|  | Sikres dataansvarlige innsyn i leverandørens taushetserklæringer ved behov? | 5.7.1 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Er det avtalt skriftlig med leverandører, i leveranser av f.eks. tjenester, maskinvare eller systemer, hvilke sikkerhetskrav som skal oppfylles for at den dataansvarlige skal kunne oppfylle sitt ansvar? | 5.7.2 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 | [ ] Ja [ ] Nei |
|  | Inkluderer avtalene forpliktelser om at partene skal oppfylle de krav og tiltak som følger av den til enhver tid gjeldende Norm for informasjonssikkerhet, samt regulering av sanksjoner ved brudd på Normen og avtalen for øvrig? | 5.7.2 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28, 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Forsikrer virksomheten, gjennom relevante avtaler, at leverandøren har tilfredsstillende internkontroll mht. sikkerhetsrevisjon og avviksbehandling? | 5.7.2 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Omfatter avtale ved tjenesteutsetting (utkontraktering) av IKT-funksjoner eller andre funksjoner av betydning for informasjonssikkerhet eller personvern minimum:* dokumentert risikovurdering som viser at tjenesteutsettende virksomhets nivå for akseptabel risiko samt Normens sikkerhetsnivå er etablert. Ved tjenesteutsetting av IKT-tjenester til andre land bør forhold ved vertslandet vurderes fordi forholdene kan påvirke risikovurderingen.
* hvilke oppgaver av sikkerhetsmessig betydning som er omfattet, og ansvarsforholdene for disse
* beskrivelse av leverandørens løsning og grensesnitt mot virksomheten i form av konfigurasjonskart
 | 5.7.3 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 32PJL § 22HRL § 21 |  |
|  | Sikrer avtale ved tjenesteutsetting at virksomheten gis rett til å revidere leverandørens aktiviteter som er knyttet til avtalen? | 5.7.3 | A.15.1.2 |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Har virksomheten en god plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av tjenesteleveransen? | 5.7.3 | A.15.2.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 32PJL § 22HRL § 21 |  |
|  | Er det avtalt ved tjenesteutsetting at ved terminering av kontrakten skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid? | 5.7.3 | A.15.1.2\*A.15.2.2\*A.8.1.4\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Er det avtalt at databehandler bare skal behandle helse- og personopplysninger etter instruks fra dataansvarlig? | 5.7.4 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 29 |  |
|  | Er det regulert i avtalen hvordan databehandler kan behandle data på vegne av dataansvarlig? | 5.7.4 | A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 (3) |  |
|  | Er det fastsatt i avtalen at dataansvarlig kun kan bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personopplysningsloven | 5.7.4 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Er det regulert i avtalen at databehandleren ikke kan engasjere underleverandører uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den dataansvarlige?  | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28(2) |  |
|  | Er det regulert i avtalen at dersom det er innhentet en generell, skriftlig tillatelse, skal databehandleren underrette den dataansvarlige om eventuelle planer for endring av underleverandører? | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 (4) |  |
|  | Er det regulert i avtalen med leverandøren at underleverandører har samme plikter som databehandler etter databehandleravtalen? | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 (4) |  |
|  | Er det avtalt at avtalen mellom leverandøren og underleverandøren skal kunne gjøres tilgjengelig for dataansvarlig? | 5.7.4.1 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Er databehandleravtalen skriftlig? | 5.7.4.2 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 (3) |  |
|  | Fremgår det av avtalen at databehandler forplikter seg til å oppfylle lovbestemte krav og kravene i Normen? | 5.7.4.2 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 |  |
|  | Fører databehandler en oversikt (protokoll) over alle kategorier av behandlingsaktiviteter som utføres på vegne av en dataansvarlig? | 5.7.4.3 | A.15.1.2\*A.15.1.3\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 30 (2) | [ ] Ja [ ] Nei |
|  | Sørger dataansvarlig for at databehandler mottar nødvendig informasjon for at databehandler kan føre en slik oversikt? | 5.7.4.3 | A.15.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 30 |  |
|  | Har databehandler, om den behandler helse- og personopplysninger fra flere virksomheter, iverksatt tekniske tiltak som ikke kan overstyres av brukerne, skiller mellom virksomhetene i henhold til gjennomført risikovurdering? | 5.7.4.4 | A.9.1\*A.9.2\*8.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Melder databehandler uten ugrunnet opphold brudd på personopplysningssikkerhet til dataansvarlig? | 5.7.4.4 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 33 (2) | [ ] Ja [ ] Nei |
|  | Har virksomheten gjennom avtale for vedlikehold, fjernaksess og fysisk service sørget for at* leverandørens utstyr som benyttes ved online oppkobling ved hjelp av kommunikasjonsnett eller medbrakt utstyr som knyttes til virksomhetens utstyr, ikke har ondsinnet programvare som inneholder virus e.l. og at utstyret er sikret mot adgang fra uvedkommende
* all tilgang og fysisk adgang skal være autorisert av virksomheten. Tilgangen skal logges og adgangen skal kontrolleres
* tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes når leverandøren utfører arbeid på virksomhetens utstyr/programvare
 | 5.7.5 | A.15.1.2\*A.6.2.2\*A.11.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 28 og 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Stiller virksomheter som tar i bruk informasjonssystemer som behandler helse- og personopplysninger krav om innebygd personvern i løsningene? | 5.7.6 | A.14.1.1\*A.14.2\*A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 25EFF § 15 |  |
|  | Har informasjonssystemene funksjonalitet som oppfyller lovbestemte og relevante krav i Normen? | 5.7.6 | A.14.1.1\*A.14.2\*A.15.1.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21EFF § 15 |  |
|  | Inngår anskaffelser, leverandøroppfølging og leverandørstyring i virksomhetens styringssystem for informasjonssikkerhet?Alle faser i leverandørstyring, fra anskaffelse til avtalen er avsluttet, skal omfattes. | 5.7.7 | A.15.1 |  |  | [ ] Ja [ ] Nei | PVF art. 28PJL § 23HRL § 22EFF § 15 |  |
|  | Sikrer virksomheten leverandøroppfølging ved:* klarhet i ansvar og roller
* at kompetanseressurser innen informasjonssikkerhet og personvern deltar i anskaffelser og leverandørstyring
* at virksomhetens ledelse (og styret hvis dette er relevant) som hovedregel involveres i beslutninger som gjelder bruk av private leverandører og/eller tjenesteutsetting av et visst omfang
 | 5.7.7 | A.15.1\*A.6.1.1\*7.2\*5.1\* |  |  | [ ] Ja [ ] Nei | PVF art. 28PJL § 23HRL § 22EFF § 15 |  |
|  | Bygger kravstilling og nødvendige sikkerhetstiltak ved bruk av leverandører på en dekkende risikovurdering? | 5.7.7 | A.14.1.1\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32 |  |
|  | Omfatter risikovurdering ved bruk av leverandører alltid scenarioer som omfatter leverandørens autoriserte og ev. uautoriserte tilgang til helse- og personopplysninger og annen taushetsbelagt informasjon? | 5.7.7 | A.15.1.1\*A.8.2\*8.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32 |  |
|  | Sikres det at relevante sikkerhetskrav inngår i alle anskaffelser? | 5.7.7 | A.14.1.1 |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32FLK § 7 |  |
|  | Sørger virksomheten for at den har tilstrekkelig bestillerkompetanse tilgjengelig? | 5.7.7 | 7.2\* |  |  | [ ] Ja [ ] Nei | PVF art. 32 |  |
|  | Passer virksomheter som overfører personopplysninger til utlandet på at beskyttelsesnivået i personopplysningsloven ikke undergraves ved overføringen? | 5.7.8 | A.13.2\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 45 | [ ] Ja [ ] Nei |
|  | Bruker virksomheten, når personopplysninger overføres til stater utenfor EU/EØS-området, såkalte «tredjeland», et av overføringsgrunnlagene i forordningen? | 5.7.8 |  |  |  | [ ] Ja [ ] Nei | PVF artikkel 45, 46, 47 |  |
|  | Har virksomheten tilstrekkelig kompetanse (f.eks. juridisk kompetanse) tilgjengelig ved overføring av opplysninger til land utenfor EU/EØS, slik at overføringen gjennomføres i tråd med regelverket? | 5.7.8 | 7.2\* |  |  | [ ] Ja [ ] Nei | PVF art. 32 |  |
|  | Gjør dataansvarlig dekkende risikovurderinger ved bruk av skytjenester og ellers følger kravene til avtaler og leverandøroppfølging i Normen? | 5.7.9 | A.15.1\*A.15.2\*8.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32 og 35FLK § 6 |  |
|  | Ivaretas følgende ved bruk av skytjenester:* ansvarsfordelingen mellom dataansvarlig og databehandler er avklart, og tilpasset leveransemodellen som benyttes
* dataansvarlig har oversikt over hvor data behandles geografisk, slik at kravene i kapittel 5.7.8 kan ivaretas
* dataansvarlig skal påse at skyleverandørens eventuelle standardavtaler ikke er i motstrid med lovbestemte krav og Normens krav
* dataansvarlig har sørget for å ha en god plan for ivaretakelse av informasjonssikkerhet og personvern ved avslutning av skytjenesten
 | 5.7.9 | A.15.1\*A.15.2\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 28 og 32 |  |
|  | Behandles uønskede hendelser (for eksempel brudd på rutiner, personvernet eller informasjonssikkerheten) som avvik? | 5.8.1 | A.16.1.4\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 33 | [ ] Ja [ ] Nei |
|  | Behandles avvik for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse? | 5.8.1 | (10.1\*,A.16.1.5\*&A.16.1.6\*) |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Har virksomheten rutiner for å oppdage og håndtere avvik? | 5.8.1 | A.16.1.1 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 5 nr. 2 og 32 FLK § 7 og 8 | [ ] Ja [ ] Nei |
|  | Dokumenteres avviksbehandlingen? | 5.8.1 | A.16.1 |  |  | [ ] Ja [ ] Nei | PVF artikkel 33 nr. 5PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Samler virksomheten inn fakta om hendelsesforløpet for etablering av korrigerende tiltak? | 5.8.1 | A.16.1 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Vurderes effekten av korrigerende tiltak og settes eventuelle andre tiltak i verk ved behov? | 5.8.1 | 10.1A.16.1.6 |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22 | [ ] Ja [ ] Nei |
|  | Gjennomføres ny risikovurdering ved alvorlige eller gjentatte avvik? | 5.8.1 | 10.1\*10.2\*8.2\* |  |  | [ ] Ja [ ] Nei | PJL § 23HRL § 22PVF artikkel 24 og 32 | [ ] Ja [ ] Nei |
|  | Sikres avviksmeldinger som inneholder personopplysninger eller informasjon med betydning for informasjonssikkerheten? | 5.8.1 | A.13.2.1 |  |  | [ ] Ja [ ] Nei | PVF art. 32PVF art. 5 nr. 1 bokstav f | [ ] Ja [ ] Nei |
|  | Rapporterer dataansvarlige avvik til Datatilsynet innen 72 timer, dersom avviket har medført brudd på personopplysningssikkerheten og har medført middels eller høy risiko for den registrerte?  | 5.8.2.1 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 33 |  |
|  | Blir den registrerte varslet om avviket dersom det er sannsynlig at avviket vil medføre høy risiko for de registrerte (pasienten/brukeren)?  | 5.8.2.2 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PJF § 14, 3. leddPVF artikkel 34 |  |
|  | Gir virksomheten den registrerte som minimum følgende informasjon:* Beskrivelse av bruddet
* Navn og kontaktinformasjon til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes
* Beskrivelse av de sannsynlige konsekvensene av bruddet
* Beskrivelse av de tiltakene som virksomheten har truffet eller foreslår å sette i gang for å håndtere bruddet, inkludert (dersom det er relevant) tiltak for å redusere eventuelle skadevirkninger som følge av bruddet
 | 5.8.2.2 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 33 og 34 |  |
|  | Varsler virksomheter som yter helse- og omsorgstjenester Statens helsetilsyn om avvik som følge av feil og avvik på informasjonssystemer?Varslingsplikten utløses * ved dødsfall eller svært alvorlig skade på pasient eller bruker
* som følge av ytelse av helse- og omsorgstjenester
* når utfallet er uventet ut fra påregnelig risiko
 | 5.8.3 | A.16.1\* |  |  | [ ] Ja [ ] Nei | HTL § 12-3 aHTIL § 6 |  |
|  | Ivaretar virksomheten følgende ved hendelser som medfører varsling til Statens helsetilsyn:* følge opp og informere pasienter og pårørende
* gjennomgå hendelsen
* identifisere og følge opp risikoreduserende tiltak
 | 5.8.3 | A.16.1\* |  |  | [ ] Ja [ ] Nei | PBL § 3-1 til 3-6 |  |
|  | Sørger virksomheten for at nødvendige helse- og personopplysninger er tilgjengelige? | 5.9 | A.17.1\*A.17.2\* |  |  | [ ] Ja [ ] Nei | PJL § 19PVF art. 32 nr. 1 bokstav b og c | [ ] Ja [ ] Nei |
|  | Har virksomheten kartlagt konsekvensen ved bortfall for å kunne etablere nødrutiner for å ivareta tilgjengelighet?Kartleggingen skal vurderes både for virksomheten som sådan og for dens autoriserte brukere. | 5.9 | A.17.1  |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Klassifiseres systemer etter følgende prioritering: * Systemer hvor stopp av tjeneste kan være kritiske, som
	+ livstruende for pasient
	+ kritisk for virksomhetens drift
* Systemer hvor stopp av tjeneste får alvorlige konsekvenser, som
	+ økt risiko for feil behandling av pasient
	+ utsettelse av utredning og behandling som kan gå ut over liv og helse
	+ betydelig merarbeid for personell
	+ tapte inntekter for virksomheten
* Systemer hvor stopp av tjeneste får moderate konsekvenser, som
	+ forsinkelser i utredning og behandling uten alvorlige helsekonsekvenser
	+ noe merarbeid for personell
	+ tapte inntekter for virksomheten
	+ redusert omdømme
	+ svekket tillit
	+ tapt effektivitet
* Systemer hvor lengre stopp kan aksepteres
* Systemer som ikke prioriteres
 | 5.9 | A.17.1\* |  |  | [ ] Ja [ ] Nei | PJL §§ 19, 1. ledd og 22HRL § 21PVF artikkel 32 | [ ] Ja [ ] Nei |
|  | Kartlegges også hvilke andre systemer og hvilken infrastruktur de klassifiserte systemene er avhengige av?Disse skal ha samme klassifisering og nivå for akseptabel risiko som for de klassifiserte systemene. | 5.9 | A.17.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 32PJL § 22HRL § 21 | [ ] Ja [ ] Nei |
|  | Har ledelsen fastsatt nivå for akseptabel risiko for tilgjengelighet for hver aktuell klassifisering, med minimum maksimal avbruddstid?  | 5.9 | A.17.1\* |  |  | [ ] Ja [ ] Nei | PJL § 22HRL § 21PVF artikkel 32FLK § 6 |  |
|  | Har virksomheten etablert nødrutiner med utgangspunkt i klassifiseringen av informasjonssystemene for:* Alternativ drift uten bruk av informasjonssystemene
* Alternativ drift med delvis støtte fra informasjonssystemene
 | 5.9 | A.17.1\* |  |  | [ ] Ja [ ] Nei | PJL §§ 19, 1. ledd, 22 og 23HRL §§ 21 og 22FLK § 7 | [ ] Ja [ ] Nei |
|  | Øves, testes, revideres og oppdateres nødrutinene minst en gang i året? | 5.9 | A.17.1\* |  |  | [ ] Ja [ ] Nei | PVF artikkel 24 og 32PJL § 22HRL § 21FLK § 8 | [ ] Ja [ ] Nei |