NORMEN Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: Direktoratet for e-helse
Sjekkliste for å kontrollere at virksomheten ivaretar kravene i Normen	**Støttedokument** **Faktaark nr 6b** Versjon: 3.7 Dato: 28.6.2019

Sjekklisten er à jour med utgave 5.3 av Normen. Dokumentet oppdateres til versjon 6.0 når den er vedtatt av styringsgruppen.

Normen krever bl.a. at det skal utarbeides en plan for gjennomføring av sikkerhetsrevisjoner. Eksempel på en revisjonsplan er å revidere områdene A. – D. nedenfor rullerende hvert 4. år:

Revisjonsområde	Delområde
A. Ledelse og ansvar	a. Ansvar og organisering av personvern og informasjonssikkerhet b. Dataansvarliges ansvar c. Styringssystemet d. Informasjonssikkerhetsmål e. Informasjonssikkerhetsinstruks f. Personvernombud g. Ledelsens gjennomgang
B. Risikostyring	a. Protokoll over behandlinger av helse- og personopplysninger b. Oversikt over IKT-utstyr c. Risikovurdering d. Personvernkonsekvensvurdering ▫ Ytterligere vurderingskriterier e. Forhåndsdrøfting med Datatilsynet
C. Personvern og pasientrettigheter	a. Taushetsplikt b. Den registrertes rettigheter: innsyn i personopplysninger og logger c. Utlevering av helse- og personopplysninger ▫ Til andre enn virksomhetens og forvaltningsorganets eget personell ▫ Til virksomhetens ledelse og til administrative systemer ▫ Til læring og kvalitetssikring
D. Informasjonssikkerhet	a. Ansatte, kompetanse og holdningsskapende arbeid ▫ Vilkår og betingelser ▫ Opplæring og kompetanse ▫ Opphør av ansettelse b. Tilgangsstyring ▫ Autorisering ▫ Autentisering ▫ Kontroll av tilgangsrettigheter c. Fysisk sikkerhet og håndtering av utstyr ▫ Nøkler/adgangskort ▫ Brukerutstyr (pc og printere - stasjonære) ▫ Driftsutstyr (servere og nettverksutstyr) ▫ Mobilt utstyr og hjemmekontor ▫ Kryptering ▫ Medisinsk utstyr d. Sikker IT-drift ▫ Konfigurasjonskontroll ▫ Sikkerhetskopiering ▫ Logging ▫ Styring og håndtering av tekniske sårbarheter

Revisjonsområde	Delområde
	▫ Sikkerhetsrevisjon av informasjonssystemer e. Kommunikasjonssikkerhet ▫ Styring av nettverkssikkerhet ▫ Sikring av nettjenester ▫ Meldingsformidling ▫ E-post, sms og sosialmedier ▫ Tilkobling til internett f. Digital kommunikasjon med pasienter/bruker g. Leverandørforhold og avtaler ▫ Leverandør av kommunikasjonstjenester ▫ Databehandler ▫ Leverandører ▫ Sikkerhetsleverandører ▫ Samarbeid mellom virksomheter om behandlingsrettede helseregistre ▫ Tilgang til helseopplysninger mellom virksomheter 39 h. Håndtering av informasjonssikkerhetsbrudd ▫ Avvikshåndtering ▫ Underretting til den registrerte i. IKT-beredskap

Forklaring til innholdet i sjekklisten nedenfor

Krav
Sjekklisten inneholder krav markert 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 sjekklisten sammen med Normen slik at kravet vurderes ift temaet som behandles i Normen.

Kap. i Normen
Det enkelte krav i sjekklisten er referert til kapittelnummer i Normen.

Kap. i ISO 27001
Det enkelte krav i sjekklisten er referert til kapittelnummer i ISO 27001.

Systemkrav i behandlingsrettet helseregister
Angir sikkerhetskrav som skal ivaretas i systemer som behandler helse- og personopplysninger (tidligere Faktaark 38). For enkelte krav er det angitt en utdypning av kravet som ikke direkte kan leses ut av Normen. Disse er angitt som ”*Utdypning av kravet*:”. Se også ”*Veiledning til systemkrav i Normen og leverandørens dokumentasjon av kravet*”.

Kravet gjelder ikke (Må begrunnes)
Normen bygger på prinsippet om forholdsmessig sikring. Ved bruk av sjekklisten må virksomheten derfor avgjøre hvilke spørsmål som er relevante, og foreta konkrete avveininger i forhold til virksomhetens størrelse. Bortfaller kravet må dataansvarlig redegjøre for hvorfor kravet utgår.

Er kravet ivaretatt
Svar om kravet er ivaretatt eller ikke.

Kraver 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.

Hjemmel i lov eller forskrift
Referanse til lov eller forskrift (med lenke) som hjemler kravet.

Felt markert med turkis gir referanse til hjemmel med følgende akronym:

- PJL: Pasientjournalloven (https://lovdata.no/dokument/NL/lov/2014-06-20-42)
- PJF: Pasientjournalforskriften (https://lovdata.no/dokument/SF/forskrift/2019-03-01-168)
- HPL: Helsepersonelloven (https://lovdata.no/dokument/NL/lov/1999-07-02-64
- PBL: Pasient- og brukerrettighetsloven (https://lovdata.no/dokument/NL/lov/1999-07-02-63)
- FEP: Forskrift om etablering og gjennomføring av psykisk helsevern (§49) (https://lovdata.no/dokument/SF/forskrift/2011-12-16-1258
- HTL: Helse- og omsorgstjenesteloven (https://lovdata.no/dokument/NL/lov/2011-06-24-30)
- HFL: Helseforskningsloven (https://lovdata.no/dokument/NL/lov/2008-06-20-44
- FIKT: Forskrift om IKT-standarder i helse- og omsorgstjenesten (https://lovdata.no/dokument/SF/forskrift/2015-07-01-853)
    - Følgende mangler i 6b, men står i Normen 5.3:
        - § 4.Krav om oppdatert adresseinformasjon mv., jf kap 5.5.3 vedr Rett adressering
        - § 5.Krav til funksjonaliteten i IKT-systemenes programvare, jf kap 5.5.3 vedr Melding eller e-post avleveres i avtalt format
- EFF: Eforvaltningsforskriften (https://lovdata.no/dokument/SF/forskrift/2004-06-25-988)
    - Med utgangspunkt i hva et forvaltningsorgan er, vurderes forskriften som ikke relevant (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."*)
- POL: Personopplysningsloven - Petter
- PVF: Personvernforordningen (GDPR) – Petter
- FLK: Forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten – Petter

Sjekkliste faktaark 6b (versjon 3.4)

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
A. LEDELSE OG ANSVAR								
1.	Er virksomheten ved avtale forpliktet til å følge Normen?	1.4				☐Ja ☐Nei		
2.	Er det den som har det overordnede ansvaret for virksomheten som etablerer og opprettholder tilfredsstillende personvern og informasjonssikkerhet?	2.1	4.4			☐Ja ☐Nei	PJL § 22 HTL § 5-10 første punktum PVF artikkel 24	
3.	Er utførelsen av oppgaver overført til eksterne (for eksempel databehandler)?	2.1				☐Ja ☐Nei	PJL §§ 22, 23	
4.	Er arbeidet med informasjonssikkerhet i virksomheten organisert og gjennomført slik at det kommer klart frem hvem som er ansvarlig på alle nivåer, og hva de er ansvarlig for?	2.1	5.3			☐Ja ☐Nei	PJL § 22 PVF artikkel 24 første ledd	☐Ja ☐Nei
5.	Omfatter arbeidet med personvern og informasjonssikkerhet styring, gjennomføring og kontroll?	2.1	6.2			☐Ja ☐Nei	PVF artikkel 24 første ledd – sikre og påse, samt gjennomgang og oppdatere? FLK §§ 3 og 4	☐Ja ☐Nei
6.	Blir personvernet og informasjonssikkerheten dokumentert i et styringssystem (internkontroll)?	2.1	7.5.1			☐Ja ☐Nei	PJL § 23 PVF artikke 24 første ledd FLK § 3	☐Ja ☐Nei
7.	Har dataansvarlig etablert et styringssystem?	2.1	4.4			☐Ja ☐Nei	PJL § 23 PVF artikkel 24 første ledd	
8.	Har databehandler etablert et styringssystem?	2.1	A.15.1.1.			☐Ja ☐Nei	PVF artikkel 28 (1)	

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
9.	Etablerer og opprettholder dataansvarlig et tilfredsstillende personvern og informasjonssikkerhet?	2.2	A.15.1.1.			☐Ja ☐Nei	PJL § 22 PVF artikkel 5 og 32	☐Ja ☐Nei
10.	Har dataansvarlig ivaretatt følgende?: • Gjennomført risikovurderinger og utarbeidet personvernkonsekvensvurdering der det er nødvendig • Etablert egnede tekniske og organisatoriske tiltak • Sikret de registrertes rett til innsyn og rett til informasjon, og ivareta reglene om retting og sletting av registrerte helse- og personopplysninger • Etablert prosedyrer for innhenting av samtykke og oppfyllelse av ev. reservasjon mot visse former for behandling av helse- og personopplysninger • Påsett og dokumentert at behandlingene er lovlige • Sender varsler ved brudd på personvernet og informasjonssikkerheten til Datatilsynet	2.2			PVF -. disse kravene er fjernet	☐Ja ☐Nei	PJL § 18 HPL §§ 41, 42, 43 og 44 PBL §§ 3-6 3. ledd, 4-1, 5-1, 5-2 PVF artikkel 32 (1), 35 (1), 13, 15, 7 og 8, 5 (1), 33,	☐Ja ☐Nei
11.	Er styringssystemet tilpasset virksomhetens størrelse, egenart og aktiviteter og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i?	2.3	5.1 a) b)			☐Ja ☐Nei	PVF artikkel 24 (1) FLK § 5	☐Ja ☐Nei
12.	Har virksomhetens øverste ledelse gjort styringssystemet kjent i virksomheten?	2.3	5.2. f)			☐Ja ☐Nei	FLK §§ 3 og 7(d)	☐Ja ☐Nei
13.	Blir dokumenter i styringssystemet holdt løpende oppdatert og arkivert fra det tidspunktet dokumentet ble erstattet med en ny gjeldende versjon?	2.3	5.2. e)			☐Ja ☐Nei	FLK § 5 (3)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
14.	Blir følgende dokumenter arkivert i minimum 5 år fra det tidspunkt dokumentet ble tatt ut av bruk?: • Alle dokumenter i styringssystemet • Resultater fra sikkerhetsrevisjoner • Resultater fra risikovurderinger • Resultater fra avviksbehandling • Referat fra ledelsens gjennomgang • Avtaler med partnere, databehandlere og leverandører	2.3				☐Ja ☐Nei	Kravet er fjernet i 6.0	☐Ja ☐Nei
15.	Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregisteret) skal oppbevares i minimum 5 år fra det tidspunkt autorisasjonen ble tatt ut av bruk?	2.3		Autorisering		☐Ja ☐Nei	Kravet er fjernet i 6.0	☐Ja ☐Nei
16.	Logger med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene, skal tas vare på til det av helsehjelpens karakter ikke lenger antas å bli bruk for.	2.3		Logging		☐Ja ☐Nei	PJL § 25	☐Ja ☐Nei
17.	Blir dokumentasjon om tiltak knyttet til informasjonssikkerhet sikret på tilsvarende måte som helse- og personopplysninger når kjennskap til tiltakene for uvedkommende vil innebære en risiko?	2.3				☐Ja ☐Nei	PJL § 22 og 23 2. ledd	☐Ja ☐Nei
18.	Har virksomheten beskrevet sikkerhetsmål i styringssystemet?	2.4		5.2.b		☐Ja ☐Nei	Efvf § 15 (1)	☐Ja ☐Nei
19.	Har virksomhetens ledelse, på bakgrunn av sikkerhetsmålene, fastsatt nivå for akseptabel risiko?	2.4		6.1.2.e.1		☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
20.	Er valgene for å oppnå informasjonssikkerhetsmålene dokumentert?	2.4		5.2.e		☐Ja ☐Nei	Efvf § 15 (1)	☐Ja ☐Nei
21.	Har virksomheten på bakgrunn av mål og valg av tiltak etablert egnede tekniske og organisatoriske tiltak?	2.4		8.1		☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
22.	Er tiltakene satt i verk på bakgrunn av en vurdering av risiko for den registrertes personvern?	2.4				☐Ja ☐Nei	PVF artikke 35 (1)	☐Ja ☐Nei
23.	Er iverksetting av tiltak for vern av personopplysninger vurdert for de forskjellige behandlingsaktivitetene?	2.4				☐Ja ☐Nei	PVF artikkel 35 (1)	☐Ja ☐Nei
24.	Har øverste ledelse sørget for at virksomheten utarbeider og forvalter en informasjonssikkerhetsinstruks som sammenfatter de vesentligste kravene til personvern og informasjonssikkerhet i virksomheten?	2.5				☐Ja ☐Nei	Efvf § 15 (1)	☐Ja ☐Nei
25.	Er instruksen tilpasset informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i?	2.5				☐Ja ☐Nei	Kravet er fjernet i 6.0	☐Ja ☐Nei
26.	Forplikter instruksen den ansatte til å følge kravene?	2.5				☐Ja ☐Nei	Kravet er fjernet i 6.0	☐Ja ☐Nei
27.	Oppdateres instruksen ved endringer i krav og tiltak?	2.5				☐Ja ☐Nei	Kravet er fjernet i 6.0	☐Ja ☐Nei
28.	Har virksomhetens øverste ledelse utpekt et personvernombud?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 37	☐Ja ☐Nei
29.	Er personvernombudet utnevnt på bakgrunn av personlige kvalifikasjoner, særlig god kompetanse på personvernlovgivning og muligheten til å utføre oppgavene?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 37 (5)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
30.	Blir personvernombudet gitt tilstrekkelige ressurser og tilgang på aktuell kompetanse til å utføre sine plikter?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 38 (2)	☐Ja ☐Nei
31.	Rapporterer personvernombudet direkte til øverste ledelse i virksomheten?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 38 (3)	☐Ja ☐Nei
32.	Har databehandler utpekt et personvernombud?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 37 (1)	☐Ja ☐Nei
33.	Er personvernombudet utnevnt på bakgrunn av personlige kvalifikasjoner, særlig god kompetanse på personvernlovgivning og muligheten til å utføre oppgavene.?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 37 (5)	☐Ja ☐Nei
34.	Arbeider personvernombudet uten interessekonflikt med eventuelle andre roller som vedkommende innehar i virksomheten, og skal ikke motta instruksjoner vedrørende hvordan oppgavene skal utføres?	2.6			PVF	☐Ja ☐Nei	PVF artiikel 37 (3) (6)	☐Ja ☐Nei
35.	Er det fastlagt at personvernombudet ikke skal beslutte behandlinger av personopplysninger eller metode/verktøy for slike behandlinger?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 39 (1)(a)	☐Ja ☐Nei
36.	Bistår personvernombudet dataansvarlig, databehandler og de ansatte i arbeidet med personvern og informasjonssikkerhet slik at nivå for akseptabel risiko blir ivaretatt?	2.6			PVF	☐Ja ☐Nei	PVF artikkel 39 (1)(b)	☐Ja ☐Nei
37.	Evaluerer virksomhetens øverste ledelse virksomhetens aktiviteter og følger opp at informasjonssikkerheten ivaretas ved minimum årlige gjennomganger?	2.7				☐Ja ☐Nei	FLK § 8(f)	☐Ja ☐Nei
38.	Blir det vedtatt tiltaksplaner for å oppnå fastsatt nivå for akseptabel risiko, med plassering av ansvar, dersom evalueringen avdekker at virkelig situasjon ikke når opp til fastsatt nivå for akseptabel risiko?	2.7	6.1.2			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
B. RISIKOSTYRING								
39.	Har både den dataansvarlige og databehandleren gjennomført forholdsmessige tekniske og organisatoriske tiltak for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet i informasjonssystemene?	3	6.1.2.c.1			☐Ja ☐Nei	PJL § 22 PVF artikkel 32 (1)(b)	☐Ja ☐Nei
40.	Er det tatt hensyn til den tekniske utviklingen, gjennomføringskostnadene og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i, ved valg av tiltakene?	3	6.2		PVF	☐Ja ☐Nei	PVF artikkel 32 (1)	☐Ja ☐Nei
41.	Er følgende overordnede krav til konfidensialitet som minimum lagt til grunn for etablering av sikkerhetstiltak?: • Personer utenfor virksomheten skal ikke kunne få uautorisert tilgang til helse- og personopplysninger. • Personer i virksomheten skal gis tilgang i henhold til fastsatte prinsipper for tilgangsstyring.	3				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
42.	Det skal registreres i logger i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har hatt tilgang.	3		Logging		☐Ja ☐Nei	PJL § 22 PJF § 14	☐Ja ☐Nei
43.	Er følgende overordnede krav til integritet som minimum lagt til grunn for etablering av sikkerhetstiltak?: • Sikkerhetstiltak skal iverksettes slik at personer eller teknologi, i eller utenfor virksomheten, ikke skal kunne endre helse- og personopplysninger uten autorisasjon.	3				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Helse- og personopplysninger skal være fullstendige og ajourført i forhold til behandlingen av opplysningene.							
44.	Helse- og personopplysninger skal være korrekte og knyttes til rett identifisert person	3		Integritet		☐Ja ☐Nei	PJF § 4, 1. ledd	☐Ja ☐Nei
45.	Helse- og personopplysninger skal føres i henhold til relevant kodeverk	3		Integritet		☐Ja ☐Nei	PJF § 6, bokstav h)	☐Ja ☐Nei
46.	Det skal registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer hvem som har foretatt registrering, endring, retting og sletting	3		Logging		☐Ja ☐Nei		☐Ja ☐Nei
47.	Er følgende overordnede krav til tilgjengelighet som minimum lagt til grunn for etablering av sikkerhetstiltak?: • Innenfor rammen av taushetsplikten skal helse- og personopplysninger være tilgjengelig når man har tjenstlige behov. • Misbruk av selvautorisering skal følges opp som avvik.	3				☐Ja ☐Nei	PJL § 19, 1. ledd PJF § 14, 3. ledd	☐Ja ☐Nei
48.	Selvautorisering kan etableres som en mulighet for autoriserte brukere til å gi seg selv tilgang uten å følge fastsatte prinsipper for å få tilgang til helse- og personopplysninger. I så tilfelle må det utarbeides egne prosedyrer for dette. Begrunnelsen for selvautorisering skal dokumenteres.	3		Autorisering		☐Ja ☐Nei		☐Ja ☐Nei
49.	Er følgende overordnede krav til robusthet som minimum lagt til grunn for etablering av sikkerhetstiltak?: • Det skal finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet,	3				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	håndtering og gjenoppretting av personopplysningssikkerheten og informasjonssikkerheten for øvrig							
50.	Er det utarbeidet en "Protokoll over behandlinger av helse- og personopplysninger" som minimum inneholder følgende opplysninger?: • Navnet på og kontaktopplysninger til den dataansvarlige og eventuelt felles dataansvarlig • Databehandlere og databehandleravtaler • Navnet på og kontaktopplysninger til personvernombud • Formålene med behandlingen • Behandlingsgrunnlag • Kategorier av registrerte (eksempelvis pasienter – barn og voksen, klient, bruker av tjenesten, ansatt, helsepersonell, bruker av informasjonssystem) • Kategorier av personopplysninger (eksempelvis ansattopplysninger, helseopplysninger) • Hvorvidt det behandles personopplysninger av særlige kategorier • Mottakere av personopplysninger (eksempelvis NAV, HELFO, reseptregisteret, forsikringsselskap, o.l.) • Eventuell overføring til utlandet og bekreftelse på at mottaker følger regulatoriske krav • Planlagt lagringstid	3.1			PVF	☐Ja ☐Nei	PVF artikkel 30	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Beskrivelse av tekniske og organisatoriske sikkerhetstiltak, jf. styringssystemet • Om det er utarbeidet personvernkonsekvensvurdering eller det er utarbeides begrunnelse for at det ikke utarbeidet							
51.	Er "Protokoll over behandlinger av helse- og personopplysninger" skriftlig?	3.1			PVF	☐Ja ☐Nei	PVF artikkel 30	☐Ja ☐Nei
52.	Har virksomheten oversikt over alt IKT-utstyr? Denne oversikten skal inkludere stasjonære og bærbare datamaskiner, mobiltelefoner og annet kommunikasjonsutstyr, servere, nettverksutstyr (rutere, svitsjer, brannmurer, osv.), skrivere, lagringsnettverk, apper, IP-telefoner mv.	3.2	A. 9.2.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
53.	Gjennomføres det risikovurderinger før behandling av helse- og personopplysninger igangsettes?	3.3	6.1.2		PVF	☐Ja ☐Nei	PVF Artikkel 32 (1)	☐Ja ☐Nei
54.	Gjennomføres det en ny risikovurdering ved endringer som har betydning for informasjonssikkerheten?	3.3	6.1.2.b			☐Ja ☐Nei	PJL § 22 PVF artikkel 32 (1)	☐Ja ☐Nei
55.	Gjennomfører virksomhetens ledelse jevnlig risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten?	3.3	6.1.2.b		PVF	☐Ja ☐Nei	PVF artikkel 32 (1)	☐Ja ☐Nei
56.	Gjennomfører dataansvarlig og databehandleren egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som står i forhold til risikoen?	3.3	8.3			☐Ja ☐Nei	PJL § 22 PVF artikkel 32(1)	☐Ja ☐Nei
57.	Identifiserer risikovurderingen behov for risikoreduserende tiltak ved å sammenligne avdekket risiko med nivå for akseptabel risiko?	3.3	6.1.2.a			☐Ja ☐Nei	PJL § 22 PVF artikkel 32 (1)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
58.	Gjennomføres risikovurdering som minimum før?: • det iverksettes behandling av helse- og personopplysninger • etablering av nye informasjonsbehandlingssystemer eller registre som inneholder helse- og personopplysninger • det iverksettes organisatoriske endringer som kan påvirke informasjonsbehandlingen • det iverksettes tekniske endringer i utstyr og/eller programvare som kan påvirke informasjonsbehandlingen • det iverksettes andre endringer med betydning for informasjonssikkerheten • det iverksettes tilgang til helseopplysninger mellom virksomheter	3.3				☐Ja ☐Nei	PVF artikkel 32 (1)	☐Ja ☐Nei
59.	Blir risikovurderingen dokumentert?	3.3	6.1.2			☐Ja ☐Nei	PJL § 23 PVF artikkel 5 (2) – se engelsk ordlyd	☐Ja ☐Nei
60.	Blir konklusjonene fra vurderingen sammenlignet med fastlagt nivå for akseptabel risiko?	3.3	6.1.2. e) 1)			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
61.	Blir det iverksatt tiltak (nye/endrede) for å oppnå akseptabel risiko om risikoen er høyere enn fastsatt nivå for akseptabel risiko?	3.3	6.1.3. a)			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
62.	Gjennomfører den dataansvarlige en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha dersom det er sannsynlig at en type behandling av helse- og	3.4			PVF	☐Ja ☐Nei	PVF artikkel 35 (1)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	personopplysninger vil medføre en høy risiko for personvernet?							
63.	Blir vurdering av personvernkonsekvenser gjennomført før behandlingen av personopplysninger starter?				PVF	☐Ja ☐Nei	PVF artikkel 35 (1)	☐Ja ☐Nei
64.	Blir personvernkonsekvensvurdering gjennomført når det medfører høy risiko for personvernet?: • ved bruk av ny teknologi • dersom behandlingens art, omfang, formål og sammenhengen den utføres i tilsier det • Konsulter Datatilsynet for liste med når personvernkonsekvensvurdering skal gjennomføres	3.4			PVF	☐Ja ☐Nei	PVF artikkel 35 (1)	☐Ja ☐Nei
65.	Gjennomføres personvernkonsekvensvurdering når behandlingen er?: • i stor skala av helseopplysninger eller av personopplysninger om straffedommer og straffbare forhold • en systematisk og omfattende vurdering av personlige aspekter ved personer basert på automatisert behandling (profilering), som danner grunnlag for avgjørelser som har rettsvirkning eller påvirker den registrerte i betydelig grad	3.4			PVF	☐Ja ☐Nei	PVF artikkel 35 (1) (b)(a)	☐Ja ☐Nei
66.	Inneholder personvernkonsekvensvurderingen minst?: • en systematisk beskrivelse av behandlingsaktivitetene • beskrivelse av formålet med behandlingen	3.4			PVF	☐Ja ☐Nei	PVF artikkel 35 (7)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• vurdering om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålet • vurdering av risikoene for personvernet til den registrerte • planlagte risikoreduserende tiltak for personvernet							
67.	Blir personvernombudet rådført ved gjennomføring av personvernkonsekvensvurderingen?	3.4			PVF	☐Ja ☐Nei	PVF artikkel 39©	☐Ja ☐Nei
68.	Blir det planlagt tiltak som reduserer risikoen for personvernet iht. personvernkonsekvensvurderingen?	3.4			PVF	☐Ja ☐Nei	PVF artikkel 35	☐Ja ☐Nei
69.	Rådfører den dataansvarlige seg med Datatilsynet om behandlingen av helse- og personopplysninger vil medføre en høy risiko som ikke kan reduseres ved hjelp av rimelige midler?	3.4			PVF	☐Ja ☐Nei	PVF artikkel 36	☐Ja ☐Nei
70.	Rådfører den dataansvarlige seg med Datatilsynet dersom?: • personvernkonsekvensvurderingen tilsier at behandlinger av helse- og personopplysninger vil medføre en høy risiko, også etter at planlagte tiltak er gjennomført • personvernkonsekvensvurderingen tilsier at behandlinger av helse- og personopplysninger vil medføre en høy risiko uansett tiltak	3.5			PVF	☐Ja ☐Nei	PVF artikkel 36	☐Ja ☐Nei
C. PERSONVERN OG PASIENTRETTIGHETER								

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
71.	Påser virksomhetens leder at alt personell som gis tilgang har taushetsplikt og at de er bevisst taushetspliktens innhold og omfang, ved å minimum?: • Beskrive konsekvenser ved brudd på taushetsplikten. • Beskrive konsekvenser ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for (ulovlig tilegnelse). • Beskrive konsekvenser ved å endre/forsøk på å endre opplysninger man ikke har autorisasjon til å endre.	4.1	A.13.2.4			☐Ja ☐Nei	PJL § 15 (delvis) HPL §§ 21 og 21 a, HTL § 12-1 HFL § 7 PBL § 3-6	☐Ja ☐Nei
72.	Fører brudd på taushetsplikten og/eller ulovlig tilegnelse som et minimum en advarsel for den som begår bruddet?	4.1	A.13.2.4			☐Ja ☐Nei	HPL § 21 a	☐Ja ☐Nei
73.	Behandles brudd på taushetsplikten og/eller ulovlig tilegnelse iht avviksprosedyre?	4.1	A.13.2.4			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei
74.	Er det etablert prosedyrer og gjennomføres det tiltak for å sikre at?: • Det innhentes skriftlig samtykke fra pasienten/brukeren i alle tilfelle hvor dette er nødvendig, herunder når tilgangen til den aktuelle behandlingen av helse- og personopplysninger ikke er fastsatt i lov eller har et annet gyldig grunnlag • Pasienten/brukeren sikres innsyn i egne helse- og personopplysninger • Pasientens/brukerens rettigheter til retting/sletting av helse- og personopplysninger ivaretas	4.2				☐Ja ☐Nei	PJL § 18 PJF §§ 11 og 15 PBL §§ 4-1, 5-1, 5-2 FEP § 49, 2. ledd (samtykke elektronisk kommunikasjon)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Pasientens rett til sperring av hele eller deler av egen pasientjournal ivaretas							
75.	Det skal etableres prosedyrer og gjennomføres tiltak for å sikre at: • Pasienten/brukeren får informasjon om virksomhetens behandling av helse- og personopplysninger, og sine rettigheter til innsyn i, retting, sletting og sperring av registrerte opplysninger om seg selv.	4.2		Pasient-rettigheter		☐Ja ☐Nei	PJL § 18	☐Ja ☐Nei
76.	Dersom den registrerte sender en anmodning elektronisk, skal informasjonen om mulig gis elektronisk	4.2		Pasient-rettigheter	PVF	☐Ja ☐Nei	PVF artikkel 15 (3)	☐Ja ☐Nei
77.	Informerer den dataansvarlige pasienten/brukeren om bruk av tilgang til helseopplysninger mellom virksomheter?	4.2				☐Ja ☐Nei	PVF artikkel 13 (1)€, 14 (1)€	☐Ja ☐Nei
78.	Blir informasjonen tilpasset pasientens/brukerens forutsetninger og tilstand, og unnlates dersom det er klart utilrådelig?	4.2				☐Ja ☐Nei	PVF artikkel 12 (1)	☐Ja ☐Nei
79.	Inneholder informasjonen blant annet: • hvilke virksomheter som gis tilgang? • hvilke helse- og personopplysninger tilgangen omfatter? • at pasienten/brukeren kan motsette seg at det gis tilgang?	4.2				☐Ja ☐Nei	PVF artikkel 13 og 14	☐Ja ☐Nei
80.	Er det etablert prosedyrer for å sikre at den registrertes rettigheter for innsyn i logger blir ivaretatt?	4.2.1				☐Ja ☐Nei	PJL § 18, 1. ledd PBL § § 5-1, 1.ledd	☐Ja ☐Nei
81.	Det skal etableres prosedyrer for å sikre at den registrertes rettigheter for innsyn i logger blir ivaretatt. Prosedyrene skal som et minimum sikre at den registrerte får informasjon om:	4.2.1		Pasient-rettigheter		☐Ja ☐Nei	PJL §§ 18, 1. ledd, 23 PJF § 14, 2. ledd (delvis) PBR § 5-1, 1.ledd, 1.punktum	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Person og organisatorisk tilhørighet til den som har behandlet helseopplysningene • Hvilke behandlinger av helse- og personopplysninger som er utført • Når behandlingene av helse- og personopplysninger er gjort.						HFL § 40, 1.ledd	
82.	Ved bruk av tilgang til helseopplysninger mellom virksomheter skal den registrerte få informasjon om: • Person og organisatorisk tilhørighet til den som har hentet fram opplysningene • Hvorfor helseopplysningene er hentet fram • Hvilke tidsperioder vedkommende har hentet fram helseopplysningene	4.2.1		Pasient-rettigheter		☐Ja ☐Nei	PVF artikkel 13 og 14	☐Ja ☐Nei
83.	Skjer overføring til annet helsepersonell enn virksomhetens eget personell, når det er nødvendig for å kunne yte forsvarlig helsehjelp, i samsvar med lovbestemte regler om taushetsplikt?	4.3.1				☐Ja ☐Nei		☐Ja ☐Nei
84.	Skjer behandlingen av forespørsel om overføring eller utlevering av helse- og personopplysninger i samsvar med prosedyrer som ivaretar kravene til konfidensialitet, integritet og tilgjengelighet?	4.3.1				☐Ja ☐Nei	PJL § 23 PVF artikkel 32	☐Ja ☐Nei
85.	Det skal fremgå av journalen når helse- og personopplysninger er gitt til annet personell enn virksomhetens eget personell	4.3.1		Pasient-rettigheter		☐Ja ☐Nei	PJL § 7	☐Ja ☐Nei
86.	Når helseopplysningene utleveres til ledelsen skal de så langt som mulig behandles uten at den registrertes navn og fødselsnummer fremgår	4.3.2		Pasient-rettigheter		☐Ja ☐Nei	HPL § 26, 1. ledd	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
87.	Blir pasienten/brukeren orientert om sin rett til å motsette seg tilgjengeliggjøring dersom det likevel er nødvendig å videreformidle personidentifiserbare opplysninger?	4.3.2				☐Ja ☐Nei	HPL § 25, 1. ledd	☐Ja ☐Nei
88.	Når helseopplysninger tilgjengeliggjøres for læring og kvalitetssikring skal de begrenses til de opplysninger som er nødvendige og relevante for formålet	4.3.3		Pasient-rettigheter		☐Ja ☐Nei	HPL § 29 c	☐Ja ☐Nei
89.	Det skal dokumenteres i pasientens journal hvilke opplysninger som er tilgjengeliggjort for ledelsen og for læring og kvalitetssikring og hvem de er tilgjengeliggjort for	4.3.3		Pasient-rettigheter		☐Ja ☐Nei	HPL § 29 c	☐Ja ☐Nei
D. INFORMASJONSSIKKERHET								
90.	Har virksomheten iverksatt tiltak som ivaretar at: • alle som gis tilgang til og/eller drifter informasjonssystemene og tilhørende informasjon har tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta informasjonssikkerheten? • alle som har tilgang til helse- og personopplysninger behandler disse etter gjeldende regelverk, Normen og virksomhetens rutiner?	5.1.2				☐Ja ☐Nei	PJL §§ 22 og 23	☐Ja ☐Nei
91.	Sørger den dataansvarlige for at, innenfor rammen av taushetsplikten, 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				☐Ja ☐Nei	PJL § 19 HPL § 25	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
92.	Sørger den dataansvarlige for at opplysningene gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten?	5.2	A. 9. 1. 1.			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
93.	Tilgangsstyring skal etableres for alle behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer?	5.2	A. 9. 1. 2.	Autorisering		☐Ja ☐Nei	PJL § 22 PJF § 13 HFL § 7, 1. ledd HPL §25, 2.ledd	☐Ja ☐Nei
94.	Tilgang til behandlingsrettede helseregistre skal gis etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten?	5.2		Autorisering		☐Ja ☐Nei		☐Ja ☐Nei
95.	Blir tilgang styrt slik at taushetspliktreglene ivaretas og at tilgang til helse- og personopplysninger ikke gis til andre enn de som har tjenstlig behov?	5.2	A.13.2.4			☐Ja ☐Nei	PJL § 22 PJF § 13, 1. ledd, a)	☐Ja ☐Nei
96.	Ved tilgang til helseopplysninger mellom virksomheter: Har begge virksomhetene tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger som minst ivaretar at: • helseopplysningene ikke gjøres tilgjengelige dersom pasienten/brukeren har motsatt seg eller motsetter seg det? • det kun gis tilgang til helseopplysninger som er relevante og nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til pasienten/brukeren? • helsepersonellet er autorisert for slik tilgang, og har autentisert seg ved bruk av sikker autentiseringsløsning?	5.2	A.9			☐Ja ☐Nei	PJL §§ 19, 22 PJF § 7, c)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
97.	Blir lovbestemt taushetsplikt vurdert og ivaretatt ved tildeling av autorisasjon?	5.2.1	A.13.2.4			☐Ja ☐Nei	PJL §§ 15, 23 PJF §§ 13, 1. ledd, a), 15	☐Ja ☐Nei
98.	Delegerer dataansvarlig myndighet for å tildele autorisasjon til den enkelte enhets ansvarlige leder?	5.2.1				☐Ja ☐Nei		☐Ja ☐Nei
99.	Tildelt autorisasjon skal sikre at den enkelte kan få tilgang til relevante og nødvendige helse- og personopplysninger i samsvar med personellets ansvar og oppgaver Utdypning av kravet: Tildelt autorisasjon skal kunne tidsavgrenses	5.2.1		Autorisering		☐Ja ☐Nei	PJL §§ 19, 22 PJL § 13, 1. ledd	☐Ja ☐Nei
100.	Benyttes det roller i virksomheten skal autorisering for hver rolle skje uavhengig av personellets øvrige roller	5.2.1	A.9.1.2	Autorisering		☐Ja ☐Nei		☐Ja ☐Nei
101.	Er det etablert prosedyre for tildeling og administrasjon av tilgangsrettigheter: • Autorisasjon for å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov. Autorisasjonen skal tildeles i henhold til betryggende prosedyrer. Lovbestemt taushetsplikt skal vurderes og overholdes. Også tekniske tiltak skal iverksettes for å ivareta krav til konfidensialitet ved aktivt å hindre uvedkommende i å få tilgang og for å sikre dokumentasjon av denne tildelte autorisasjon?	5.2.1	A.9.2			☐Ja ☐Nei	PJL §§ 22 og 23 PJF § 13 HPL §§ 25, 1. ledd og 2. ledd	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger. Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes? • Autorisasjon for andre tjenester gis etter tjenstlig behov, f.eks. autorisasjon til bruk av e-post, bruk av Internett e.l?							
102.	Det skal registreres i det behandlingsrettede helseregisteret (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes.	5.2.1		Logging		☐Ja ☐Nei	PJF § 14, c)	☐Ja ☐Nei
103.	Autorisasjon for å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger skal gis til dem som har tjenstlig behov	5.2.1		Autorisering		☐Ja ☐Nei	PJF §§ 13, 1.ledd og bokstav a)	☐Ja ☐Nei
104.	Kun teknisk personell med særskilt behov for tilgang, kan autoriseres for større mengder helse- og personopplysninger	5.2.1		Autorisering		☐Ja ☐Nei		☐Ja ☐Nei
105.	Det skal iverksettes tiltak slik at mulig misbruk skal kunne avdekkes	5.2.1		Autorisering		☐Ja ☐Nei	PJL § 22 PJL § 14, 3. ledd	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
106.	Er følgende tiltak iverksatt for å hindre at personer uten autorisasjon får tilgang til helse- og personopplysninger: • Tekniske og organisatoriske tiltak skal iverksettes slik at personer ikke skal kunne få tilgang til helse- og personopplysninger de ikke er autorisert for? • Dersom det er åpnet for selvautorisering, skal tekniske tiltak etableres på en slik måte at helsepersonell kan få tilgang til nødvendige helse- og personopplysninger. Slik tilgang skal grunngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))?	5.2.1	A.9.2			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
107.	Tekniske tiltak skal iverksettes slik at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystem hvem som har endret og hva som er endret Utdypning av kravet der det ikke benyttes PKI: Passordfil skal krypteres	5.2.1	A.9.2	Autentisering		☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
108.	Systemet som administrerer autorisasjon skal skille mellom rettigheter til å lese, registrere, rette, slette og/eller sperre helse- og personopplysninger	5.2.1	A.9.2	Autorisering		☐Ja ☐Nei	PJL § 22 PJF § 13, 1. ledd HPL § 25, 1. ledd	☐Ja ☐Nei
109.	All tildeling av autorisasjon skal registreres i et autorisasjonsregister	5.2.1	A.9.2	Autorisasjon		☐Ja ☐Nei	PJF 13, 1.ledd, c)	☐Ja ☐Nei
110.	Dersom det er åpnet for selvautorisering, skal tekniske tiltak etableres på en slik måte at	5.2.1		Autorisering		☐Ja ☐Nei	PJL § 19, 2. ledd	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	helsepersonell kan få tilgang til nødvendige helse- og personopplysninger							
111.	Tilgang ved selvautorisering skal grunngis og registreres i behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ))	5.2.1		Autorisering		☐Ja ☐Nei	PJL § 19, 2. ledd	☐Ja ☐Nei
112.	Misbruk av selvautorisering skal følges opp som avvik	5.2.1		Autorisering		☐Ja ☐Nei	PJF § 14, 3. ledd	☐Ja ☐Nei
113.	Dataansvarlig skal sørge for at det opprettes et autorisasjonsregister. Registeret skal 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) Utdypning av kravet: Det skal også registreres hvem (fysisk identifiserbar person) som har opprettet (registrert) autorisasjonen	5.2.1.1		Autorisering		☐Ja ☐Nei	PJL § 22 PJF § 13, 1.ledd c)	☐Ja ☐Nei
114.	Har dataansvarlig for nasjonal kjernejournal delegert myndighet for å tildele autorisasjon til den enkelte virksomhet som skal ta i bruk kjernejournal?	5.2.1.2				☐Ja ☐Nei		☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
115.	Skjer autorisasjon til kjernejournal gjennom autorisasjonsløsning i egen virksomhet?	5.2.1.2				☐Ja ☐Nei		☐Ja ☐Nei
116.	Er autorisasjonen til kjernejournal tidsbegrenset?	5.2.1.2				☐Ja ☐Nei		☐Ja ☐Nei
117.	Ved tilgang til helseopplysninger mellom virksomheter: Blir følgende ivaretatt ved helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet: • beskrive rettigheter og plikter som følger av autorisasjonen? • være i samsvar med regler om taushetsplikt? • dokumenteres i virksomhetens autorisasjonsregister? • alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold?	5.2.1.3				☐Ja ☐Nei	PJF § 13, 1. ledd	☐Ja ☐Nei
118.	Ved tilgang til helseopplysninger mellom virksomheter skal autorisasjonen tidsbegrenses	5.2.1.3		Autorisering		☐Ja ☐Nei	PJF § 13, 1. ledd, bokstav b) og c)	☐Ja ☐Nei
119.	Ved tilgang til helseopplysninger mellom virksomheter skal det være en funksjon for å sperre tilgang til helseopplysninger for helsepersonell fra andre virksomheter Med sperring menes en teknisk løsning der hele eller deler av journalen gjøres utilgjengelige for helsepersonell. Opplysningene skal kunne sperres overfor både enkeltpersoner, grupper av helsepersonell og virksomheter.	5.2.1.3		Pasient-rettigheter		☐Ja ☐Nei	PJL § 17 PJF § 13, 1. ledd pasient- og brukerrettighetsloven §§ 4-3 til 4-7	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
120.	Ivaretar autentiseringen minimum følgende: • Tildeling av autentiseringskriteria (som brukernavn og passord) skal gjennomføres på en betryggende måte? • Tilgang fra hjemmekontor og/eller mobilt utstyr skal sikres ved autentisering som ikke innebære økt risiko utover det som gjelder for stasjonært utstyr?	5.2.2				☐Ja ☐Nei	PJL § 22 PJF § 13, 2. ledd	☐Ja ☐Nei
121.	Ved tilgang til behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer skal ulike ansettelsesforhold identifiseres.	5.2.2	A.9	Autentisering		☐Ja ☐Nei		☐Ja ☐Nei
122.	Flere personer skal ikke benytte samme autentiseringskriteria. Utdypning av kravet 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	Autentisering		☐Ja ☐Nei	PJF § 13, 2. ledd	☐Ja ☐Nei
123.	Om det benyttes roller skal den enkelte rolle identifiseres	5.2.2	A.9.1.2	Autentisering		☐Ja ☐Nei		☐Ja ☐Nei
124.	Om det benyttes roller skal den enkelte rolle ved behov gis ulike autentiseringskriteria	5.2.2	A.9.1.2	Autentisering		☐Ja ☐Nei		☐Ja ☐Nei
125.	Foretar den enkelte leder gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner:	5.2.3	A.9			☐Ja ☐Nei	PJL § 22 og 23 PJF § 13, 1. ledd bokstav e) og 3. ledd	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• 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?							
126.	Virksomhetens ledelse skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister (inkl elektronisk pasientjournal (EPJ)) eller i et fagsystem. Utdypning av kravet: Behandlingsrettet helseregister inkl elektronisk pasientjournal (EPJ) eller fagsystem må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	5.2.3	A.9.4	Autorisering		☐Ja ☐Nei	PJF § 13, 1. ledd bokstav e) og 3. ledd	☐Ja ☐Nei
127.	Blir virksomhetens ledelse varlet dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang?	5.2.3	A.12.4.1			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei
128.	Blir hendelsen behandlet iht. etablerte prosedyrer for avviksbehandling, særlig med henblikk på å få avklart om eksisterende tilgangskontroll er god nok?	5.2.3	A.12.4.1			☐Ja ☐Nei	PJL § 23 PVF artikkel 33	☐Ja ☐Nei
129.	Blir Datatilsynet informert dersom kontrollen viser at det har skjedd en urettmessig tilgang?	5.2.3				☐Ja ☐Nei	PVF artikkel 33	☐Ja ☐Nei
130.	Vurderer virksomhetens ledelse om pasienten/brukeren skal informeres?	5.2.3				☐Ja ☐Nei	PJF § 14, 3. ledd PVF artikkel 34	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
131.	Samarbeider avtalepartene ved bruk av tilgang til helseopplysninger mellom virksomheter om kontroll av tilganger?	5.2.3				☐Ja ☐Nei		☐Ja ☐Nei
132.	Ved tilgang til helseopplysninger mellom virksomheter skal dataansvarlige, som har adgang til å autorisere helsepersonell for tilgang, løpende kontrollere: - 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		Autorisering		☐Ja ☐Nei		☐Ja ☐Nei
133.	Blir pasienten/brukeren varslet, av virksomheten opplysningene er hentet fra, om kontrollen viser at noen urettmessig har hentet frem helseopplysninger?	5.2.3				☐Ja ☐Nei		☐Ja ☐Nei
134.	Blir avviket behandlet iht. etablerte prosedyrer for avviksbehandling?	5.2.3	A.12.4.1			☐Ja ☐Nei	PJL § 23 PVF artikkel 33	☐Ja ☐Nei
135.	Er det etablert prosedyre for administrasjon av nøkler/adgangskort i adgangskontrollsystemet?	5.3.1	A.11.1.2			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei
136.	Er det etablert sikkerhetstiltak som hindrer at personer som ikke er autoriserte får tilgang til helse- og personopplysninger – enten ved adgangsregulert kontroll av lokaler med utstyr, eller ved at utstyret sikres mot misbruk og skjermer, utskrifter mv. skjermes mot uautorisert innsyn?	5.3.2	A.11.1			☐Ja ☐Nei	PJL §§ 22, 23	☐Ja ☐Nei
137.	Er det etablert sikkerhetstiltak som hindrer at annet enn autorisert personell får adgang til driftsutstyr?	5.3.3	A.11.1.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
138.	Blir alle lagringsmedia, dvs. disker, minnepinne, CD, mv., merket, og alle helse- og personopplysninger slettet når lagringsmediet tas ut av bruk?	5.3.3	A.8			☐Ja ☐Nei	PJL § 22 PVF artikkel 17	☐Ja ☐Nei
139.	Blir det gjennomført risikovurdering av løsningene som benyttes for mobilt utstyr og hjemmekontor?	5.3.4				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
140.	Er det etablert administrative prosedyrer for bruk av mobilt utstyr og hjemmekontor?	5.3.4	A.8.1			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei
141.	Er det ved bruk av mobilt utstyr og hjemmekontor etablert sikkerhetstiltak som hindrer at personer som ikke er autorisert får tilgang til helse- og personopplysninger ved at: • Tekniske tiltak iverksettes slik at det kun kan kommuniseres med predefinert utstyr. Autentisering skal ikke innebære økt risiko utover det som gjelder for stasjonært utstyr. En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet? • Helse- og personopplysninger skal bare lagres lokalt når dette er nødvendig ut fra tjenstlig behov og skal alltid lagres kryptert? • All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer sikres ved kryptering iht. «NSM Cryptographic Requirements Version 3.1»[1]?	5.3.4	A.8			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

[1] https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
142.	Er det iverksatt tekniske tiltak slik at all kommunikasjon av helse- og personopplysninger utenfor virksomhetens kontroll krypteres?	5.3.5	A.10.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
143.	Blir lagringsenhet for medisinsk utstyr som behandler helse- og personopplysninger plassert i avlåst rom eller i bemannet område?	5.3.6	A.11.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
144.	Blir medisinsk utstyr som behandler helse- og personopplysninger inkludert i virksomhetens arbeid med informasjonssikkerhet, herunder i risikovurderinger, tilgangsstyring og prosedyrer for bruk, på linje med andre informasjonssystemer?	5.3.6	A.11.1			☐Ja ☐Nei	PJL § 22 Håndteringsforskriften § 11?	☐Ja ☐Nei
145.	Blir konfigurasjonen sikret slik at utstyret og programvaren kun utfører de funksjoner som er formålsbestemt?	5.4.1				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
146.	Blir følgende gjennomført før konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, blir satt i drift: • 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				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
147.	Blir konfigurasjonskontroll regulert gjennom avtale ved: • Bruk av databehandler?	5.4.1				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Bruk av fjernaksess for vedlikehold og oppdateringer?							
148.	Blir alle endringer i organisasjonen, informasjonssystemene og systemer som har innvirkning på informasjonssikkerheten forankret på relevant ledernivå?	5.4.2	5.1			☐Ja ☐Nei		☐Ja ☐Nei
149.	Har virksomheten utarbeidet prosedyrer for endringsledelse som tar opp i seg følgende temaer: • Identifisering av vesentlige endringer? • Planlegging og testing av endringer? • Vurdering av potensielle konsekvenser, for eksempel ved å gjennomføre en risikovurdering? • Godkjennelsesprosedyre for endringer? • Kommunikasjon av plan til aktuelle personer/roller? • Reserveprosedyrer om endringen må avbrytes, feiler eller at uønskede hendelser oppstår? • Endringslogg med relevante opplysninger?	5.4.2	9.3			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei
150.	Sørger virksomhetens ledelse for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk?	5.4.3	A.12.3.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
151.	Blir sikkerhetskopier oppbevart avlåst og brannsikret, og adskilt fra driftsutstyret?	5.4.3	A.12.3.1			☐Ja ☐Nei		☐Ja ☐Nei
152.	Blir det jevnlig foretatt test av at sikkerhetskopiene er korrekte og kan tilbakeføres?	5.4.3	A.12.3.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
153.	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
154.	Er det etablert prosedyrer for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke?	5.4.4	A.12.4			☐Ja ☐Nei	PJL § 23	☐Ja ☐Nei
155.	Et det etablert prosedyrer for ved behov å kunne sammenholde loggene med autorisasjonsregister?	5.4.4	A.12.4			☐Ja ☐Nei		☐Ja ☐Nei
156.	Fører brudd som avdekkes til at personalmessige reaksjoner iverksettes?	5.4.4	A.7.2.3			☐Ja ☐Nei		☐Ja ☐Nei
157.	Blir det iverksatt nødvendige tekniske tiltak dersom personalmessige reaksjoner ikke har nødvendig effekt over tid, dvs. det er gjentatt tilgang av flere personer som ikke er autorisert?	5.4.4				☐Ja ☐Nei		☐Ja ☐Nei
158.	Blir det, for å oppdage brudd eller forsøk på å bryte regelverket, som minimum ført logg over følgende: • Sikkerhetsbarrierene skal registrere sikkerhetsrelevante hendelser, bl.a. forsøk på uautorisert bruk av informasjonssystemet? • Nettverksoperativsystemer skal registrere alle forsøk på uautorisert bruk?	5.4.4				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
159.	For å oppdage brudd eller forsøk på å bryte regelverket skal det som minimum føres logg over: • Autorisert bruk av informasjonssystemene skal registreres.	5.4.4		Logging		☐Ja ☐Nei	PJF § 14, 1. og 3. ledd	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Alle informasjonssystemer skal registrere alle forsøk på uautorisert bruk. • Bruk av selvautorisering til behandlingsrettet helseregister skal registreres.							
160.	Logger skal sikres mot endring og sletting av uautorisert personell	5.4.4		Logging		☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
161.	Følgende skal som minimum registreres i loggene: • entydig identifikator for den autoriserte brukeren • rollen den autoriserte brukeren har ved tilgangen (om det benyttes roller) • virksomhetstilhørighet • organisatorisk tilhørighet til den som er autorisert • type opplysninger det er gitt tilgang til • hvem som har fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer • grunnlaget for tilgangen • tidspunkt og varighet for tilgangen	5.4.4		Logging		☐Ja ☐Nei	PJF § 14, 1. ledd (kun delvis) HPL § 45, 1. ledd	☐Ja ☐Nei
162.	Ved tilgang til helseopplysninger mellom virksomheter skal i tillegg følgende logges: • person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene • hvorfor helseopplysningene er hentet frem • hvilke tidsperioder vedkommende har hentet frem helseopplysningene	5.4.4		Logging		☐Ja ☐Nei		☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
163.	Alle logger skal kunne analyseres ved hjelp av egnet verktøy og ved behov sammenholdes med autorisasjonsregister	5.4.4	A.12.4	Logging		☐Ja ☐Nei		☐Ja ☐Nei
164.	Har virksomheten prosedyrer for å skaffe seg informasjon om tekniske sårbarheter i utstyr og programvare?	5.4.5	A.12.6.1			☐Ja ☐Nei	PJL § 23, 1. ledd	☐Ja ☐Nei
165.	Er det etablert prosedyrer 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	8.1			☐Ja ☐Nei	PJL § 23, 1. ledd	☐Ja ☐Nei
166.	Foreligge det en godkjent plan for sikkerhetsrevisjoner?	5.4.6	9.2			☐Ja ☐Nei	PJL § 23, 1. ledd PVF artikkel 32 (1)(d)	☐Ja ☐Nei
167.	Omfatter sikkerhetsrevisjonen som minimum vurderinger av: • Plassering av ansvar og organisering av sikkerhetsarbeidet? • Kvalitet på sikkerhetsmål og sikkerhetsstrategi? • Overholdelse av prosedyrer for bruk av informasjonssystemer og helse- og personopplysninger? • Resultat av opplæring? • Forvaltning og bruk av helse- og personopplysninger? • Tilgang til helse- og personopplysninger og tiltak mot uautorisert innsyn?	5.4.6	9.2			☐Ja ☐Nei	PJL § 22, 1. ledd (ansvar og organisering, tilgangsstyring) PJL § 23 (kontroll)	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Testing, analysering og vurdering av hvor effektive de tekniske og organisatoriske sikkerhetstiltak er? • Ivaretakelse av informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og leverandører?							
168.	Blir resultatene og konklusjonene fra sikkerhetsrevisjonene dokumentert?	5.4.6	9.2.g			☐Ja ☐Nei	PJL § 23, 2. ledd	☐Ja ☐Nei
169.	Blir sikkerhetsrevisjonen som avdekker bruk av informasjonssystemene som ikke er forutsatt, behandlet som avvik?	5.4.6				☐Ja ☐Nei	PJL § 23, 1. ledd	☐Ja ☐Nei
170.	Har virksomheten tydelig definert hvilke krav som gjelder for nettverkssikkerhet, og er tiltakene som iverksettes basert på en risikovurdering?	5.5.1	6.1			☐Ja ☐Nei	PJL § 22, 1. ledd	☐Ja ☐Nei
171.	Er det etablert tekniske tiltak ved tilkobling til nett utenfor virksomheten som ivaretar at: • Kun eksplisitt angitt tillatt trafikk kan passere, annet stoppes? • Minst to uavhengige, tekniske tiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne få uautorisert tilgang til og/eller kunne endre eller slette helse- og personopplysninger? • Trafikk kan ikke passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra virksomhetens systemer? • Logging iverksettes for å kontrollere at regler ikke brytes; ved brudd stenges kanalen inntil ny sikker løsning finnes?	5.5.2	A.13.1			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
172.	Har virksomheten iverksatt tiltak for å forhindre at helseopplysninger tilgjengeliggjøres ved hjelp av e-post, SMS eller andre ukrypterte kanaler: • Virksomheten skal forsikre seg om ved tekniske tiltak og organisatoriske tiltak at e-post ikke inneholder identifiserbare helseopplysninger? • Logging skal iverksettes for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik og personalmessige konsekvenser skal vurderes?	5.5.4				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
173.	Har virksomheten iverksatt følgende tiltak: • Tekniske tiltak som sikrer at Internett-tjenesten er logisk atskilt fra der helse- og personopplysninger behandles? • Logging iverksettes for å kontrollere at regler ikke brytes. Regelbrudd skal håndteres som avvik og personalmessige konsekvenser skal vurderes?	5.5	A.8.2 (og A.12.4.1).			☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei
174.	Er det inngått skriftlige avtaler med kommunikasjonsparter dersom ikke annet er angitt?	5.7	A.15.1.1.			☐Ja ☐Nei		☐Ja ☐Nei
175.	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				☐Ja ☐Nei		☐Ja ☐Nei
176.	Er det avtalt at databehandler bare skal behandle helse- og personopplysninger etter instruks fra dataansvarlig?	5.7.2				☐Ja ☐Nei	PVF artikkel 28	

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
177.	Er det regulert i avtale hvordan databehandler behandler data på vegne av dataansvarlig?	5.7.2				☐Ja ☐Nei	PVF artikkel 28 (3)	
178.	Er det regulert at databehandleren ikke kan engasjere underleverandører uten at det på forhånd er innhentet særlig eller generell skriftlig tillatelse til dette fra den dataansvarlige?	5.7.2.1	A.15			☐Ja ☐Nei	PVF artikkel 28(2)	
179.	Er det regulert at dersom det er innhentet en generell, skriftlig tillatelse, skal databehandleren underrette den dataansvarlige om eventuelle planer for endring av underleverandører?	5.7.2.1	A.15.2.2.			☐Ja ☐Nei	PVF artikkel 28 (4)	
180.	Er databehandleravtalen skriftlig?	5.7.2.3	A.15.1.1.			☐Ja ☐Nei	PVF artikkel 28 (3)	
181.	Fremgår det av avtalen at databehandler forplikter seg til å oppfylle kravene i Normen?	5.7.2.3				☐Ja ☐Nei		
182.	Beskriver databehandleravtalen: • Databehandlers oppgaver? • Hensikten med behandlingen av helse- og personopplysninger? • Varigheten av behandlingen? • Behandlingens formål og art? • Typen personopplysninger? • Kategorier av registrerte? • Dataansvarliges rettigheter og plikter?	5.7.2.3				☐Ja ☐Nei	PVF artikkel 28	
183.	Regulerer databehandleravtalen: • Konkrete sikkerhetstiltak? • Databehandler skal på eget initiativ treffe alle tiltak som er nødvendig for å sikre god informasjonssikkerhet, herunder å følge kravene i Normen?	5.7.2.3				☐Ja ☐Nei	PVF artikkel 28	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Databehandler skal bare kunne overføre personopplysningene til utlandet etter instruks fra den dataansvarlige? • Databehandler skal bare autorisere personer som er underlagt taushetsplikt for behandling av helse- og personopplysninger? • Krav til bruk av underleverandører (annen databehandler)? • Dataansvarlig skal sikres innsynsrett for å forsikre seg om at kravene etterleves?							
184.	Regulerer databehandleravtalen at databehandler har plikt til å bistå med/i: • tekniske og organisatoriske tiltak for å utøve den registrertes rettigheter? • relevante tekniske og organisatoriske tiltak for å sikre god informasjonssikkerhet? • å melde brudd på personvernet til Datatilsynet? • å varsle den registrerte om brudd på personvernet? • dokumentasjon av allerede gjennomført relevant personvernkonsekvensvurdering eller gjennomføring av? personvernkonsekvensvurdering • forhåndsdrøftinger med Datatilsynet • slette eller tilbakelevere? personopplysningene etter instruks • gjøre tilgjengelig all informasjon som viser at pliktene etter databehandleravtalen er ivaretatt? • å bidra i sikkerhetsrevisjoner?	5.7.2.3				☐Ja ☐Nei	PVF artikkel 28	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• å bidra i inspeksjoner? • endring av instrukser fra den dataansvarlige som er i strid med lovverket?							
185.	Har databehandler, som også er en leverandør av et system eller en tjeneste som krever en personvernkonsekvensvurdering, fremlagt dette eller bistått med å utarbeide dette?	5.7.2.3				☐Ja ☐Nei	PVF artikkel 28 (3) (h)	☐Ja ☐Nei
186.	Fører databehandler en protokoll over alle kategorier av behandlingsaktiviteter som utføres på vegne av en dataansvarlig som inneholder: • Navnet på og kontaktopplysningene til databehandleren? • Navnet på dataansvarlig som databehandleren opptrer på vegne av? • Dataansvarliges personvernombud? • Kategoriene av behandling utført på vegne av hver dataansvarlig? • Overføring av personopplysninger til utlandet? • Beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene?	5.7.2.4				☐Ja ☐Nei	PVF artikkel 30 (2)	☐Ja ☐Nei
187.	Er oversikten skriftlig?	5.7.2.4				☐Ja ☐Nei	PVF artikkel 30	☐Ja ☐Nei
188.	Har databehandler, om den behandler helse- og personopplysninger fra flere virksomheter, iverksatt tekniske tiltak som ikke kan overstyres av brukerne, ivaretatt at det er etablert skiller mellom virksomhetene i henhold til gjennomført risikovurdering?	5.7.2.5				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
189.	Melder databehandler uten ugrunnet opphold brudd på personopplysningssikkerhet til dataansvarlig?	5.7.2.5				☐Ja ☐Nei	PVF artikkel 33 (2)	☐Ja ☐Nei
190.	Forsikrer virksomheten seg, for å ivareta konfidensialitet, integritet og tilgjengelighet for helse- og personopplysningene, at: • leverandørens personale har undertegnet taushetserklæring som innebærer en absolutt taushetsplikt med henblikk på alle helse- og personopplysninger? • leverandøren etterlever Normen med tanke på dataansvarliges plikter vedrørende sikkerhetsrevisjoner og avviksbehandling? • 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? • leverandøren kun skal få adgang etter særskilt tillatelse fra virksomheten i hvert enkelt tilfelle, og kun adgang til de enheter hvor det er behov? • all adgang skal skje under overvåking fra virksomhetens personale? • tilgjengelighet til helse- og personopplysninger så vidt mulig skal opprettholdes når leverandøren utfører arbeid på virksomhetens utstyr/programvare, slik at virksomhetens oppgavebehandling ivaretas?	5.7.3				☐Ja ☐Nei	PJL § 22	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
191.	Er det inngått avtale med en sikkerhetsleverandør om gjennomføring av konkrete sikkerhetsoppgaver hvor følgende er avtalefestet: • Hvilke sikkerhetsoppgaver som er omfattet og ansvarsforholdene for disse? • Beskrivelse av leverandørens løsning i form av konfigurasjonskart? • Dokumentert risikovurdering som viser at virksomhetens nivå for akseptabel risiko samt Normens sikkerhetsnivå er etablert?	5.7.4				☐Ja ☐Nei		
192.	Er det, om to eller flere virksomheter samarbeider om felles journal som skal erstatte virksomhetenes interne journal, inngått skriftlig avtale om: • hva samarbeidet omfatter? • hvordan pasientens eller brukerens rettigheter skal ivaretas? • hvordan helseopplysningene skal behandles og sikres, også ved endringer i eller opphør av samarbeidet? • databehandlingsansvaret?	5.7.5				☐Ja ☐Nei	PJL § 9	
193.	Er kommunen dataansvarlig, når en kommune og en eller flere private tjenesteytere som yter tjenester på vegne av kommunen tar i bruk felles journal for å oppfylle journalføringsplikten?	5.7.5				☐Ja ☐Nei	HTL § 3-1	
194.	Er avtalen ved tilgang til helseopplysninger mellom virksomheter skriftlig og minst angir: • hva avtalen gjelder? • hvilke behovs- og risikovurderinger som ligger til grunn for avtalen?	5.7.6				☐Ja ☐Nei		

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• hvilke behandlingsrettede helseregistre, deler av registre eller typer av opplysninger avtalen omfatter? • rutiner og fordeling av oppgaver for å ivareta kravene i forskriften?							
195.	Gjennomfører begge virksomhetene risikovurdering for å påse at pasienten/brukerens personvern ivaretas når det åpnes for tilgang til helseopplysninger mellom virksomheter?	5.7.6				☐Ja ☐Nei	PVF artikkel 32	
196.	Omfatter risikovurderingene risiko for brudd på taushetsplikten og svekket informasjonssikkerhet?	5.7.6				☐Ja ☐Nei		
197.	Har virksomhetens ledelse, eller det organ ledelsen bemyndiger, rutiner for å behandle avvik med det formål å gjenopprette normal tilstand, fjerne årsaken til avviket og å hindre gjentagelse?	5.8.1	10.1.a og 10.1.b			☐Ja ☐Nei	PJL § 23, 1. ledd	☐Ja ☐Nei
198.	Blir det for hvert rapportert avvik foretatt en innsamling av fakta om hendelsesforløpet og foretatt en vurdering som grunnlag for iverksettelse av korrigerende tiltak?	5.8.1	10.1			☐Ja ☐Nei		☐Ja ☐Nei
199.	Blir det foreslått tiltak og eventuelle alternative tiltak med beskrivelse av plan for gjennomføring for å gjenopprette normal tilstand og forhindre gjentagelse?	5.8.1	10.1			☐Ja ☐Nei		☐Ja ☐Nei
200.	Blir tiltak og plan på det nivå som er gjennomførbart vedtatt slik at tiltaket hindrer eller reduserer sannsynligheten for gjentagelse?	5.8.1	10.1			☐Ja ☐Nei	PVF artikkel 32	☐Ja ☐Nei
201.	Blir det ved gjentatte avvik gjennomført en ny risikovurdering?	5.8.1	10.1 og 10.2			☐Ja ☐Nei		☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
202.	Sender den dataansvarlige melding om avvik, som har medført brudd på personvernet og konsekvenser for den registrerte, til Datatilsynet innen 72 timer etter å ha fått kjennskap til det?	5.8.1				☐Ja ☐Nei	PVF artikkel 33	

203.	Inneholder meldingen til Datatilsynet:
	• beskrivelse av bruddet på personopplysningssikkerheten inklusive
	  ○ kategorier av registrerte som er berørt?
	  ○ omtrentlig antall registrerte som er berørt?
	  ○ hvilke typer personopplysninger bruddet omfatter?
	• navnet på og kontaktopplysningene til personvernombudet eller annen kontakt der mer informasjon kan innhentes?
	• beskrivelse av de sannsynlige konsekvensene av avviket?
	• beskrivelse av tiltak den dataansvarlige har iverksatt eller foreslår å iverksette for å håndtere og redusere eventuelle skadevirkninger av avviket?
		5.8.1				☐Ja ☐Nei	PVF artikkel 33	

204.	Blir den registrerte varslet om avviket har medført sletting, endring eller uautorisert tilgjengeliggjøring/tilgang til helse- og personopplysninger?	5.8.2				☐Ja ☐Nei	PJF § 14, 3. ledd PVF artikkel 34	
205.	Inneholder varselet: • Beskrivelse av bruddet på alminnelig språk? • Kontaktopplysningene til personvernombudet eller en annen rolle som kan gi nærmere informasjon?	5.8.2				☐Ja ☐Nei	PVF artikkel 34	

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Beskrivelse av de sannsynlige konsekvensene av avviket? • Beskrivelse av gjennomførte og/eller planlagte tiltak for å håndtere og redusere skadevirkninger?							

206.	Blir systemer med tilhørende helse- og personopplysninger som virksomheten benytter, klassifisert som:
	• Systemer hvor stopp av tjeneste kan være kritiske, for eksempel
	  ○ livstruende for pasient
	  ○ kritisk for virksomhetens drift
	• Systemer hvor stopp av tjeneste får alvorlige konsekvenser? f.eks. kan medføre
	  ○ feilbehandling av pasient
	  ○ betydelig merarbeid for personell
	  ○ tapt effektivitet
	  ○ tapte inntekter for virksomheten
	• Systemer hvor stopp av tjeneste kan føre til svekkelse av pasientens tillit?
	• Systemer hvor lengre stopp kan aksepteres.
	• Systemer som ikke prioriteres?
		5.9				☐Ja ☐Nei	PJL §§ 19, 1. ledd og 22	☐Ja ☐Nei

207.	Blir det kartlagt hvilke andre systemer de klassifiserte systemene er avhengige av? Disse skal ha samme klassifisering og nivå for akseptabel risiko som de kritiske systemene	5.9				☐Ja ☐Nei		☐Ja ☐Nei
208.	Har ledelsen fastsatt nivå for akseptabel risiko for tilgjengelighet for hver aktuell klassifisering, med minimum en maksimal avbruddstid?	5.9				☐Ja ☐Nei		☐Ja ☐Nei
209.	Har virksomheten etablert nødprosedyrer med utgangspunkt i klassifiseringen av informasjonssystemene:	5.9				☐Ja ☐Nei	PJL §§ 19, 1. ledd, 22 og 23	☐Ja ☐Nei

Nr	Krav	Kap. i Normen	Kap. i ISO 27001	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 (lenke til hjemmel)	Kravet blir ivaretatt av data-behandler
	• Alternativ drift uten bruk av informasjonssystemene? • Alternativ drift med delvis støtte fra informasjonssystemene?							
210.	Blir disse prosedyrene minimum testet årlig?	5.9				☐Ja ☐Nei		☐Ja ☐Nei
211.	Vurderer virksomhetens ledelse, iht. klassifiseringen ovenfor å etablere alternativ løsning som sikrer kontinuitet av informasjonssystemene ved uforutsett driftsstans?	5.9	A.17.1			☐Ja ☐Nei	PJL § 19, 1. ledd	☐Ja ☐Nei