

 <p style="text-align: center;">Norm for informasjonssikkerhet www.normen.no</p>	<p>Utgitt med støtte av:</p> <p> Direktoratet for e-helse</p>
<h2>Sikkerhetsrevisjon</h2> <h3>Sjekkliste for å ivareta kravene i Normen</h3>	<p>Støttedokument Faktaark nr 6b Versjon: 2.1 Dato: 4.7.2016</p>

Sjekklisten er à jour med utgave 5.2 av Normen.

Sjekklisten inneholder kravene 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.

Det er kun krav markert med ”skal” i Normen som er med i sjekklisten.

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.

Det enkelte krav i sjekklisten nedenfor er referert til med kapittelnummer i Normen.

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 hvert 4. år:

År	Revisjonsområde	Tema
1.	A.	Administrativ og organisatorisk sikkerhet (roller, prosedyrer, kontroller)
2.	B.	EPJ/fagsystem (sikkerhetskrav og bruk/tilgang til helseopplysninger)
3.	C.	Fysisk sikring (av datarom, plassering av skrivere og skjermer, osv)
4.	D.	Teknisk løsning (nettverk, tilgang eksterne nett, sikkerhetsmekanismer, drift, prosedyrer, sikkerhetskopi, avtaler, osv)

Sjekklisten nedenfor er inndelt med følgende områder:

- A. Administrativ og organisatorisk sikkerhet (roller, prosedyrer, kontroller)
- B. EPJ/fagsystem (sikkerhetskrav og bruk/tilgang til helseopplysninger)
- C. Fysisk sikring (av datarom, plassering av skrivere og skjermer, osv)
- D. Teknisk løsning (nettverk, tilgang eksterne nett, sikkerhetsmekanismer, drift, prosedyrer, sikkerhetskopi, avtaler, osv)

Kolonnen ”Kravet blir ivaretatt av databehandler” 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 databehandlingsansvarlig og databehandler skal ivareta er markert med **grønt**.

Sjekkliste:

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
A. Administrativ og organisatorisk sikkerhet (roller, prosedyrer, kontroller)					
1.	Er virksomheten underlagt kravene i Normen? (iht avtale med Norsk Helsenettet SF eller annen avtale)	1.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
2.	Er det sendt melding/søkt om konsesjon til Datatilsynet for alle behandlinger av helse- og personopplysninger?	3.1 og 3.2.	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
3.	Fornytes alle meldinger til Datatilsynet hvert 3. år?	3.1 og 3.2.	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
4.	Har virksomhetens leder avklart at behandlinger av helse- og personopplysninger virksomheten foretar er lovlige?	3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
5.	Er ledelsen klar over sitt ansvar som databehandlingsansvarlig?	3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
6.	Er ansvar og oppgaver for informasjonssikkerhet dokumentert (i et organisasjonskart)?	3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
7.	Er ansvar og oppgaver beskrevet på alle nivåer?	3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
8.	Er ansvarsforholdene gjort kjent i organisasjonen?	3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
9.	Er alle sikkerhetstiltak dokumentert (organisatoriske, fysiske og tekniske)?	3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
10.	Sikres dokumentasjon av tiltak knyttet til informasjonssikkerhet på tilsvarende måte som helse- og personopplysninger?	3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
11.	Er alle styrende, gjennomførende og kontrollerende dokumenter oppdatert?	3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
12.	Arkiveres alle styrende, gjennomførende og kontrollerende dokumenter i minimum 5 år fra det tidspunktet dokumentet ble erstattet med en ny gjeldende utgave?	3.3.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
13.	Arkiveres følgende dokumenter i minimum 5 år?: <ul style="list-style-type: none"> Resultater fra sikkerhetsrevisjoner Resultater fra risikovurderinger Resultater fra avviksbehandling Referat fra ledelsens gjennomgang Oversikt over tildelte autorisasjoner og tilganger til helse- og personopplysninger (autorisasjonsregister) Avtaler med partnere, databehandlere og leverandører 	3.3.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
14.	Arkiveres logger med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene, til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem?	3.3.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
15.	Arkiveres tilstedeværelsesregister som er relevante ift kontroll mot autorisasjonsregistre og logger til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem?	3.3.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
16.	Er det etablert et styringssystem for informasjonssikkerhet?	4.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
17.	Er sikkerhetsmål for virksomheten fastsatt?	4.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
18.	Er følgende sikkerhetsmål innarbeidet? Helse – og personopplysninger skal: <ul style="list-style-type: none"> • Være tilgjengelig for rett personell til rett tid i henhold til fastsatte prinsipper for tilgangsstyring • Behandles i tråd med reglene om taushetsplikt og være beskyttet slik at uvedkommende ikke får kjennskap til opplysningene. Uvedkommende omfatter også personell som ikke har tjenstlig behov • Være fullstendige, oppdaterte og korrekte og et resultat av rettmessige registreringer og kontrollerte aktiviteter. • Begrenses slik at kun det som er nødvendig av helse- og personopplysninger behandles. 	4.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
19.	Er formålene med behandlingene av helse- og personopplysninger dokumentert?	4.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
20.	Er overordnede føringer for virksomhetens bruk av informasjonsteknologi dokumentert?	4.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
21.	Er sikkerhetsstrategi for å nå sikkerhetsmålene utarbeidet?	4.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
22.	Er nivå for akseptabel risiko for konfidensialitet, tilgjengelighet, integritet og kvalitet dokumentert? Vær oppmerksom på at minimumskravene til nivå for akseptabel risiko er angitt i kapitlene 4.4.1 til 4.4.3	4.4, 4.4.1, 4.4.2, 4.4.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
23.	Er det utarbeidet en samlet oversikt over alle behandlinger av helse- og personopplysninger i virksomheten?	4.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
24.	<p>Inneholder oversikt over alle behandlinger av helse- og personopplysninger minimum:</p> <ul style="list-style-type: none"> • Kategorier av helse- og personopplysninger • Formålet med behandlingene • Juridisk hjemmelsgrunnlag for behandlingene • Angivelse av system/register/utstyr, og om det er elektronisk eller manuelt • Grunnlaget for behandlingene • Om opplysningene er sensitive eller ikke-sensitive. Helseopplysninger er alltid sensitive personopplysninger • Konesjonsplikt/meldeplikt/hjemmel for unntak • Evt. partnere, databehandlere eller leverandører • Internt ansvarlig for det enkelte system/register/utstyr 	4.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
25.	Er det utarbeidet en plan for gjennomføring av risikovurderinger?	3.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
26.	<p>Er det gjennomført og dokumentert risikovurderinger av alle behandlinger av helse- og personopplysninger?</p> <p>Risikovurdering skal som minimum gjennomføres før:</p> <ul style="list-style-type: none"> • 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 	4.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
27.	Er resultatet av risikovurderingene sammenlignet med fastlagt nivå for akseptabel risiko?	4.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
28.	Inneholder risikovurderingene dokumentasjon av risikoreducerende tiltak?	4.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
29.	Gjennomfører virksomhetens ledelse jevnlig risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten?	4.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
30.	Er det etablert prosedyre for oppfølging av resultater fra risikovurderingene?	3.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
31.	Har databehandler gjennomført risikovurdering for å dokumentere skille mellom flere virksomheter når databehandler er databehandler for flere virksomheter? <i>Benyttes ikke databehandler angis svaret IR = Ikke relevant.</i>	5.8.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
32.	Er det gjennomført risikovurdering før tilgang til helseopplysninger mellom virksomheter tas i bruk og dekker den minimum brudd på taushetsplikten og svekket informasjonssikkerhet? <i>Benyttes ikke tilgang til helseopplysninger mellom virksomheter angis svaret IR = Ikke relevant.</i>	5.8.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
33.	Er det gjennomført risikovurdering av hjemmekontor?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
34.	Er det gjennomført risikovurdering av mobilt utstyr?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
35.	Er det etablert administrative prosedyrer for bruk av hjemmekontor?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
36.	Er det etablert administrative prosedyrer for bruk av mobilt utstyr?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
37.	Er alle medarbeidere informert om sin taushetsplikt og klar over dens innhold og omfang?	5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
38.	Er konsekvenser ved brudd på taushetsplikten beskrevet?	5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
39.	Er konsekvenser ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for beskrevet?	5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
40.	Er konsekvenser ved å endre/forsøk på å endre opplysninger man ikke har autorisasjon til å endre beskrevet?	5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
41.	Behandles brudd på taushetsplikten og/eller ulovlig tilegnelse iht. avvikprosedyre?	5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
42.	Behandles regelbrudd ved sending av e-post med sensitive personopplysninger som avvik?	5.7.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
43.	Vurderes personalmessige konsekvenser ved sending av e-post med sensitive personopplysninger?	5.7.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
44.	Behandles regelbrudd ved bruk av Internett som avvik?	5.7.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
45.	Vurderes det personalmessige konsekvenser ved brudd på bruk av Internett?	5.7.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
46.	Er det gjennomført tilstrekkelige tiltak for å sikre at meldinger sendes til rett mottaker i SMS-løsning for påminnelse om timeavtale og annet administrativt innhold?	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
47.	Er det lagt til rette for at pasient/bruker kan melde fra til virksomheten om at de ikke ønsker å motta slike meldinger?	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
48.	Er autorisasjon og tilgang kun gitt til personell som er underlagt virksomhetens instruksjonsmyndighet eller til personell som arbeider under instruksjonsmyndighet av virksomhetens eventuelle databehandlere?	5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
49.	Er autorisasjon bare gitt i den grad det er nødvendig for vedkommendes arbeid, er begrunnet i tjenstlige behov og er i henhold til bestemmelser om taushetsplikt?	5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
50.	Er det etablert tilgangsstyring for alle behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer?	5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
51.	Vurderes og ivaretas lovbestemt taushetsplikt ved tildeling av autorisasjon?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
52.	Tildeles autorisasjonen i henhold til betryggende prosedyrer?	5.2.2	<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nei		<input checked="" type="checkbox"/> Ja <input type="checkbox"/> Nei
53.	Har databehandlingsansvarlig delegert myndighet for å tildele autorisasjon til den enkelte enhets ansvarlige leder?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
54.	Er det bare autorisert personell som kan få tilgang til helse- og personopplysninger?	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
55.	Utleveres eller gis helse- og personopplysninger til annet helsepersonell enn virksomhetens eget personell i samsvar med lovbestemte regler om taushetsplikt?	5.2.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
56.	Behandles forespørsel om overføring, utlevering eller tilgang til helse- og personopplysninger i samsvar med betryggende prosedyrer?	5.2.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
57.	Er det etablert prosedyrer for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke?	5.2.8 5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
58.	Iverksettes personalmessige reaksjoner dersom brudd avdekkes?	5.2.8	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
59.	Er det etablert prosedyrer for ved behov å kunne sammenholde loggene med autorisasjonsregister og tilstedeværelsesregister?	5.2.8 5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
60.	Er det utarbeidet og iverksatt prosedyrer for behandling av helse- og personopplysninger?	5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
61.	Er det etablert prosedyrer for bruk av papirutskriften?	3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
62.	Behandles brudd på prosedyrer som avvik?	5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
63.	Er det etablert prosedyre slik at det ikke søkes annen informasjon enn den man er autorisert for og har behov for i den aktuelle arbeidssituasjon?	5.3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
64.	Er det etablert prosedyre for nødrettstilgang?	5.3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
65.	Følges all bruk av nødrettstilgang opp som avvik?	5.3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
66.	Er det etablert regler for beskyttelse av autentiseringskriteria (bl.a. ved hemmeligholdelse av passord)?	5.3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
67.	Er det etablert rutiner og organisatoriske tiltak som sikrer at alle helse- og personopplysninger som registreres er relevante og nødvendige?	5.3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
68.	Registreres all informasjon snarest mulig etter at den har fremkommet?	5.3.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
69.	Kontrolleres tilgangsstyring, herunder tildelte autorisasjoner, ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde?	5.3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
70.	Kontrolleres tilgangsstyring minimum årlig (gjørne i forbindelse med sikkerhetsrevisjon)?	5.3.2 6.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
71.	Kontrolleres tilgangsstyring ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet?	5.3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
72.	Får pasienten informasjon om virksomhetens behandling av helse- og personopplysninger, og sine rettigheter til innsyn i, retting, sletting og sperring av hele/deler av egen journal?	5.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
73.	Innhentes det samtykke fra pasienten 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?	5.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
74.	Informeres pasienten/brukeren om bruk av tilgang til helseopplysninger mellom virksomheter? Informasjonen skal blant annet inneholde <ul style="list-style-type: none"> • hvilke virksomheter som gis tilgang • hvilke helse- og personopplysninger tilgangen omfatter • at pasienten/brukeren kan motsette seg at det gis tilgang 	5.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
75.	Er det etablert prosedyrer som sikrer at den registrerte får innsyn i logger og minimum får informasjon om?: <ul style="list-style-type: none"> • hvem som har hatt tilgang eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer • hvor ofte tilgangen er benyttet 	5.3.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
76.	<p>Er det etablert prosedyrer som sikrer at den registrerte får innsyn i logger ved bruk av tilgang til helseopplysninger mellom virksomheter som gir informasjon om?:</p> <ul style="list-style-type: none"> • person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene • hvorfor helseopplysningene er hentet frem • hvilke tidsperioder vedkommende har hentet frem helseopplysningene 	5.3.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
77.	Er det etablert avtale med ansvarsforhold mellom avsender, mottaker og eventuell meldingsformidler for bruk av meldingsformidling og e-post som inneholder sensitive personopplysninger?	5.7.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
78.	<p>Er det avtalt at avsender er ansvarlig for:</p> <ul style="list-style-type: none"> • Egen tilkoblingssikring som hindrer utilsiktet utlevering og inntrenging? • Tjenesten skal ikke kunne formidle program som inneholder virus e.l.? • Sikker overføringskryptering ende-til-ende? • Rett adressering? • Ved behov skal meldingen eller e-posten være signert på en slik måte at virksomheten ikke kan benekte å ha sendt den? • Avviksrapportering i forbindelse med feilsending? • Melding eller e-post avleveres i avtalt format? 	5.7.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
79.	<p>Er det avtalt at mottaker er ansvarlig for:</p> <ul style="list-style-type: none"> • Egen tilkoblingssikring som hindrer utilsiktet utlevering og inntrenging? • Ivareta overføringskryptering ende-til-ende? • Ved behov skal mottaket registreres slik at mottaker ikke kan benekte å ha mottatt meldingen eller e-posten? • Avviksrapportering i forbindelse med feil, dvs. mottak av melding eller e-post som ikke er adressert til virksomheten? • Melding eller e-post mottas i avtalt format? 	5.7.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
80.	Er det avtalt at meldingsformidler er ansvarlig for: <ul style="list-style-type: none"> Melding eller e-post kun avleveres til adressaten? Melding eller e-post skal ikke endres eller destrueres under transport fra avsender til mottaker? Melding eller e-post skal ikke kunne leses av andre enn avsender og mottaker? Melding eller e-post skal avleveres innen avtalte tidsfrister fra avsendelse? Avviksrapportering i forbindelse med alle ovenstående punkter? 	5.7.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
81.	Er det iverksatt tiltak som ivaretar at alle som bruker og/eller drifter informasjonssystemene og tilhørende informasjon har tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta informasjonssikkerheten?	5.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
82.	Er det innhentet samtykke fra pasienten/brukeren for å formidle helse- og personopplysninger elektronisk? Dersom pasient/bruker har oppgitt digital kontaktinformasjon anses dette som et samtykke.	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
83.	Gjennomføres det sikkerhetsrevisjon jevnlig og minimum årlig?	6.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
84.	Foreligger det en plan for sikkerhetsrevisjoner?	6.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
85.	Dekker sikkerhetsrevisjonen minimum?: <ul style="list-style-type: none"> 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 Effekten av etablerte sikkerhetstiltak Ivaretagelse av informasjonssikkerhet hos kommunikasjonspartnere, databehandlere og leverandører 	6.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
86.	Dokumenteres resultatet av sikkerhetsrevisjonene?	6.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
87.	Er det etablert prosedyre for oppfølging av resultatet (avvik) av sikkerhetsrevisjoner?	3.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
88.	Behandles bruk av informasjonssystemene som ikke er forutsatt som avvik?	6.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
89.	Er det etablert prosedyre for behandling av avvik?	6.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
90.	Er alle medarbeidere klar over ansvaret de har for å melde avvik?	6.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
91.	Rapporteres behandling av avvik til ledelsen i virksomheten?	6.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
92.	Er det etablert prosedyre som sikrer at Datatilsynet varsles ved uautorisert utlevering av helse- og personopplysninger?	6.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
93.	Gjennomføres ledelsens gjennomgang minimum årlig?	6.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
94.	Dekker ledelsens gjennomgang minimum?: <ul style="list-style-type: none"> • Resultat fra sikkerhetsrevisjoner • Resultat fra risikovurderinger • Resultater fra avviksbehandling. Virksomhetens ledelse skal regelmessig følge opp at tiltak på grunnlag av avvik fastlegges, planlegges og gjennomføres • Ansvarsforhold og organisering mht. sikkerhet • Formål med behandling av helse- og personopplysninger og oversikt over helse- og personopplysninger som behandles i virksomheten • Konfigurasjonskart over informasjonssystemene. • Sikkerhetsmål, nivå for akseptabel risiko og strategier for informasjonssikkerhet • Kontroll og oppfølging av inngåtte avtaler 	6.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
95.	Dokumenteres resultatet av ledelsens gjennomgang?		<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
96.	Vedtas det tiltaksplaner dersom ledelsens gjennomgang avdekker at virkelig situasjon ikke når opp til fastsatt nivå for akseptabel risiko?	6.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
97.	Er det etablert prosedyre for oppfølging av handlingsplaner besluttet av ledelsen?	3.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
98.	Kontrollerer virksomhetens ledelse jevnlig hvem som har hatt elektronisk tilgang til helseopplysninger i et behandlingsrettet helseregister (inkl elektronisk pasientjournal (EPJ)) eller i et fagsystem	6.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
99.	Gjennomføres løpende kontroll, ved bruk av tilgang til helseopplysninger mellom virksomheter, av?: <ul style="list-style-type: none"> • hvem i egen virksomhet som elektronisk har hentet frem helseopplysninger fra annen virksomhet • hvorfor dette er gjort • tidsperioden helseopplysningene er hentet frem <i>Benyttes ikke tilgang til helseopplysninger mellom virksomheter angis svaret IR = Ikke relevant</i>	6.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
100.	Varsles, ved bruk av tilgang til helseopplysninger mellom virksomheter, virksomheten opplysningene er hentet fra og pasienten/brukeren opplysningene gjelder ved urettmessig tilgang til helseopplysninger? <i>Benyttes ikke tilgang til helseopplysninger mellom virksomheter angis svaret IR = Ikke relevant</i>	6.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
101.	Er det inngått avtale med kommunikasjonsleverandør iht kravene i Normen? Norsk Helsenett er en kommunikasjonsleverandør. <i>Benyttes ikke kommunikasjonsleverandør angis svaret IR = Ikke relevant.</i>	5.8.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
102.	Er det inngått avtale med databehandler iht kravene i Normen? <i>Benyttes ikke databehandler kan svaret IR = Ikke relevant angis.</i>	5.8.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
103.	Er konfigurasjonskontroll regulert gjennom avtale med databehandler? <i>Benyttes ikke databehandler angis svaret IR = Ikke relevant.</i>	5.5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
104.	Er det inngått avtale med leverandør iht kravene i Normen? <i>Benyttes ikke leverandør angis svaret IR = Ikke relevant.</i>	5.8.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
105.	Er det ved bruk av fjernaksess for vedlikehold og oppdateringer fra leverandør, regulert konfigurasjonskontroll gjennom avtale? <i>Benyttes ikke leverandør angis svaret IR = Ikke relevant.</i>	5.5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
106.	Er det inngått avtale med sikkerhetsleverandør iht kravene i Normen? <i>Benyttes ikke sikkerhetsleverandør angis svaret IR = Ikke relevant.</i>	5.8.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
107.	Er det inngått avtale om samarbeid mellom virksomheter om felles journal iht kravene i Normen? <i>Benyttes ikke samarbeid mellom virksomheter om behandlingsrettede helseregistre angis svaret IR = Ikke relevant.</i>	5.8.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
108.	Er det inngått avtale om tilgang til helseopplysninger mellom virksomheter iht kravene i Normen? <i>Benyttes ikke tilgang til helseopplysninger mellom virksomheter angis svaret IR = Ikke relevant.</i>	5.8.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
109.	Er det ved tilgang til helseopplysninger mellom virksomheter etablert følgende prosedyrer; krav til risikovurdering, fysisk sikring, organisering, sikkerhetsrevisjon og avvikshåndtering? <i>Benyttes ikke tilgang til helseopplysninger mellom virksomheter angis svaret IR = Ikke relevant.</i>	5.8.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
110.	Påses det at virksomheter som gis tilgang til helseopplysninger oppfyller kravene til informasjonssikkerhet? <i>Benyttes ikke tilgang til helseopplysninger mellom virksomheter angis svaret IR = Ikke relevant.</i>	5.8.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
B. EPJ/Fagsystem (sikkerhetskrav og bruk/tilgang til helseopplysninger)					
111.	Tildeles autentiseringskriteria (som brukernavn og passord) på en betryggende måte?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
112.	Har alle brukere unike autentiseringskriteria?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
113.	Sikrer autentiseringen av brukeren identifisering i korrekt rolle i hvert enkelt tilfelle?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
114.	Identifiseres den enkelte brukers ulike roller og gis de ved behov ulike autentiseringskriteria?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
115.	Identifiseres ulike ansettelsesforhold ved tilgang til behandlingsrettede helseregistre (inkl elektronisk pasientjournal (EPJ)) og fagsystemer?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
116.	Er det gjennomført risikovurdering for å påse at autentiseringen er tilfredsstillende?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
117.	Autoriseres bruker selvstendig for hver enkelt rolle?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
118.	Sikrer autentisering ved bruk av mobilt utstyr, hjemmekontor og trådløs kommunikasjon samme risikonivå som for stasjonært utstyr?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
119.	Benyttes sikker autentiseringsløsning ved tilgang til helseopplysninger mellom virksomheter?	5.2.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
120.	Er det opprettet et autorisasjonsregister som minimum inneholder?: <ul style="list-style-type: none"> informasjon om hvem som er tildelt autorisasjon til hvilken rolle autorisasjonen er tildelt 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) 	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
121.	Registreres all tildeling av autorisasjon i autorisasjonsregisteret?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
122.	Autoriseres personer som har ulike roller i virksomheten for hver rolle uavhengig av vedkommendes øvrige roller?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
123.	Skiller systemet som administrerer autorisasjon mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
124.	Gis autorisasjon for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger til dem som har tjenstlig behov?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
125.	Autoriseres kun teknisk personell med særskilt behov for tilgang til større mengder helse- og personopplysninger?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
126.	Er det iverksatt tiltak for å hindre at teknisk personell misbruker sin autorisasjon?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
127.	Tildeles autorisasjon for andre tjenester, f.eks. bruk av e-post og Internett etter tjenstlig behov?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
128.	Ivaretas det at helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet: <ul style="list-style-type: none"> beskriver rettigheter og plikter som følger av autorisasjonen er i samsvar med regler om taushetsplikt dokumenteres i virksomhetens autorisasjonsregister tidsbegrenses alltid vurderes og eventuelt endres når det oppstår endringer i ansvarsområder eller ansettelsesforhold 	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
129.	Ivaretas det at pasienten/brukeren kan kreve at tilgang til egne helseopplysninger sperrer for helsepersonell fra andre virksomheter enn der opplysningene er nedtegnet? (Ved tilgang til helseopplysninger mellom virksomheter)	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
130.	Registreres det i behandlingsrettet helseregister (inkl elektronisk pasientjournal (EPJ)) eller fagsystemet når autorisasjonen benyttes?	5.2.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
131.	Gis tilgang først etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten?	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
132.	Styres tilgang slik at taushetspliktreglene ivaretas og at tilgang til helse- og personopplysninger ikke gis til andre enn de som har tjenstlig behov?	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
133.	Ivaretas kravet i spørsmål 131. også i akuttstiasjoner som ikke er å regne som nødrettstilgang?	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
134.	Fremgår det av journalen, der reglene om taushetsplikt krever det, at tilgang i akuttstiasjon er gitt?	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
135.	Fremgår det av journalen når helse- og personopplysninger er gitt til annet helsepersonell enn virksomhetens eget personell?	5.2.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
136.	Fremgår det av journalen hvilke opplysninger som er utlevert og hvem de er utlevert til når de utleveres til læring og kvalitetssikring?	5.2.6	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		
137.	Gis tilgang til fagsystemer på bakgrunn av beslutninger om tjenstlig behov?	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
138.	Har begge virksomhetene, ved tilgang til helseopplysninger mellom virksomheter, tekniske og organisatoriske løsninger som avgrenser tilgangen til helseopplysninger som minst ivaretar at?: <ul style="list-style-type: none"> 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 	5.2.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
139.	Benyttes datasystemene bare til pålagte oppgaver?	5.2.7	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
140.	Brukes datasystemene for privat brev/dokumentskrivning, utveksling av privat e-post m.m. i bare den grad dette ikke utsetter helse- og personopplysninger for risiko?	5.2.7	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
141.	Lagres registeret over autorisert bruk og forsøk på uautorisert bruk så lenge at det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for det?	5.2.8	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
142.	Kan loggene enkelt analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd?	5.2.8	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
143.	Er det iverksatt nødvendige tekniske tiltak hvis personalmessige reaksjoner ikke har hatt nødvendig effekt over tid? Dvs. det er gjentatt tilgang av flere personer som ikke er autorisert.	5.2.8	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
144.	Er logger, autorisasjonsregister og tilstedeværelsesregister sikret mot endring og sletting av uautorisert personell?	5.2.8 5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
145.	Er pasienten sikret innsyn i egne helse- og personopplysninger?	5.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
146.	Er pasientens rettigheter til retting/sletting av helse- og personopplysninger ivaretatt?	5.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
147.	Er pasientens rett til sperring av hele eller deler av egen journal ivaretatt?	5.3.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
148.	Er det etablert tekniske tiltak slik at helsepersonell i nødrettssituasjoner, kan få tilgang til nødvendige helse- og personopplysninger (nødrettstilgang)?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
149.	Må bruk av nødrettstilgang grunngis og registreres i EPJ-systemet?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
150.	Logges bruk av nødrettstilgang?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
151.	Behandles bruk av nødrettstilgang som avvik?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
152.	Har alle systemer mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
C. Fysisk sikring (av datarom, plassering av skrivere og skjermer, osv)					
153.	Er det etablert prosedyre for administrasjon av nøkler/adgangskort i adgangskontrollsystemet?	5.4.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
154.	Er brukerutstyr (arbeidsstasjon, PC og skrivere) sikret slik at kun personer som er autoriserte får tilgang til helse- og personopplysninger?	5.4.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
155.	Er det etablert sikkerhetstiltak slik at kun autorisert personell får adgang til driftsutstyr (servere og nettverksutstyr)?	5.4.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
156.	Er lagringsenhet for elektromedisinsk utstyr som behandler helse- og personopplysninger plassert i avlåst rom eller i bemannet område?	5.4.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
D. Teknisk løsning (nettverk, tilgang eksterne nett, sikkerhetsmekanismer, drift, prosedyrer, sikkerhetskopi, avtaler, osv)					
157.	Er det utarbeidet konfigurasjonskart over informasjonssystemene?	3.3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
158.	Er det utarbeidet teknisk beskrivelse av konfigurasjonen?	3.3.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
159.	Er det iverksatt tekniske tiltak slik at hjemmekontor kun kan kommuniseres med predefinert utstyr?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
160.	Er det iverksatt tekniske tiltak slik at mobilt utstyr kun kan kommuniseres med predefinert utstyr?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
161.	Er tilgang fra avdelingskontor som kommuniserer ved hjelp av linjer man ikke har fysisk kontroll over, hjemmekontor og/eller mobilt utstyr, sikret ved autentisering som ikke innebærer økt risiko utover det som gjelder for stasjonært utstyr? En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet.	5.4.4 5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
162.	Lagres helse- og personopplysninger lokalt kun når det er tjenstlig behov?	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
163.	Er helse- og personopplysninger som lagres lokalt på mobilt utstyr kryptert iht gjeldende krav? Se. "Kravspesifikasjon for PKI i offentlig sektor".	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
164.	Er helse- og personopplysninger som lagres lokalt på hjemmekontor kryptert iht gjeldende krav? Se. "Kravspesifikasjon for PKI i offentlig sektor".	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
165.	Er all kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer kryptert iht gjeldende krav? Se. "Kravspesifikasjon for PKI i offentlig sektor".	5.4.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
166.	Er elektromedisinsk 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?	5.4.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
167.	Har virksomheten oversikt over og kontroll på alt utstyr og programvare (inklusive utstyr ved avdelingskontor og hjemmekontor og mobilt utstyr) som benyttes i behandlingen av helse- og personopplysninger?	5.5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
168.	Utfører konfigurasjonen av utstyret og programvaren kun de funksjoner som er formålsbestemt (ref strategi og mål)?	5.5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
169.	Settes konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, først i drift når følgende tiltak er gjennomført? <ul style="list-style-type: none"> 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 	5.5.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
170.	Er det iversatt minst to uavhengige tekniske tiltak slik at personer utenfor virksomheten ikke skal kunne få tilgang til og/eller kunne endre eller slette helse- og personopplysninger?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
171.	Krypteres all kommunikasjon av helse- og personopplysninger som foregår utenfor virksomhetens kontroll?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
172.	Er det iverksatt tekniske og organisatoriske tiltak slik at personer innenfor virksomheten ikke skal kunne få tilgang til helse- og personopplysninger de ikke er autorisert for?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
173.	Er det etablert tekniske tiltak slik at personer innenfor 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?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
174.	Er det iverksatt to uavhengige tekniske tiltak slik at uautorisert programvare ikke skal kunne endre helse- og personopplysninger?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
175.	Er alle lagringsmedia, dvs. disketter, CD-ROM mv., merket?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
176.	Slettes alle helse- og personopplysninger når lagringsmediet tas ut av bruk?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
177.	Overholdes plikten til arkivering av opplysningene når lagringsmediet tas ut av bruk?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
178.	Logges autorisert bruk av informasjonssystemene?	5.2.8 5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
179.	Logges sikkerhetsrelevante hendelser i sikkerhetsbarrierene, bl.a. forsøk på uautorisert bruk av informasjonssystemet?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
180.	Logges alle forsøk på uautorisert bruk av nettverksoperativsystemer?	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
181.	Logges alle forsøk på uautorisert bruk av alle informasjonssystemer?	5.2.8 5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
182.	Inneholder loggene minimum?: <ul style="list-style-type: none"> • entydig identifikator for den autoriserte brukeren • rollen den autoriserte brukeren har ved tilgangen • virksomhetstilhørighet • organisatorisk tilhørighet til den som er autorisert • hvilke 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 	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
183.	Logges i tillegg følgende ved bruk av tilgang til helseopplysninger mellom virksomheter?: <ul style="list-style-type: none"> • person og organisatorisk tilhørighet til den som har hentet frem helseopplysningene • hvorfor helseopplysningene er hentet frem • hvilke tidsperioder vedkommende har hentet frem helseopplysningene 	5.5.2	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
184.	Er informasjonssystemene som er kritiske for virksomheten kartlagt?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
185.	Er informasjonssystemene som benyttes til behandling av helse- og personopplysninger klassifisert?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
186.	Er det kartlagt hvilke andre systemer de klassifiserte systemene er avhengige av og har de samme klassifisering og nivå for akseptabel risiko som de kritiske systemene?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
187.	Er det for hver klassifisering fastsatt maksimal avbruddstid?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
188.	Er det på grunnlag av klassifiseringen etablert nødprosedyrer for alternativ drift uten bruk av informasjonssystemene?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
189.	Er det på grunnlag av klassifiseringen etablert nødprosedyrer for alternativ drift med delvis støtte fra informasjonssystemene?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
190.	Testes prosedyrene for alternativ drift minimum årlig?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
191.	Har virksomhetens ledelse, iht. klassifiseringen ovenfor, vurdert å etablere alternativ løsning som sikrer kontinuitet av informasjonssystemene ved uforutsett driftsstans?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
192.	Har virksomhetens ledelse sørget for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
193.	Oppbevares sikkerhetskopier avlåst?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
194.	Oppbevares sikkerhetskopier brannsikret?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
195.	Oppbevares sikkerhetskopier adskilt fra driftsutstyret?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
196.	Foretas det jevnlig test at sikkerhetskopiene er korrekte?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
197.	Foretas det jevnlig test at sikkerhetskopiene kan tilbakeføres?	5.5.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
198.	Ved tilkobling til nett utenfor virksomheten: Er det etablert tekniske tiltak som sikrer at kun eksplisitt angitt trafikk kan passere og annen stoppes?	5.7.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
199.	Ved tilkobling til nett utenfor virksomheten: Er det etablert tekniske tiltak som sikrer at trafikk ikke kan passere direkte utenfra og inn, men at all slik ekstern trafikk må initieres fra virksomhetens systemer?	5.7.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
200.	Ved tilkobling til nett utenfor virksomheten: Er det etablert logging slik at det er mulig å kontrollere at regler ikke brytes? Ved brudd på reglene skal kanalen stenges inntil ny sikker løsning finnes.	5.7.1	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
201.	Har virksomheten iverksatt tiltak for å forhindre at sensitive personopplysninger utleveres ved hjelp av e-post?	5.7.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
202.	Har virksomheten forsikret seg om ved tekniske tiltak og organisatoriske tiltak at e-post ikke inneholder sensitive personopplysninger?	5.7.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
203.	Er det iverksatt logging for bruk av e-post for å kontrollere at regler ikke brytes?	5.7.3	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
204.	Er det iverksatt tekniske tiltak som sikrer at Internett-tjenesten er logisk atskilt fra der helse- og personopplysninger behandles?	5.7.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
205.	Er det iverksatt logging for å kontrollere at regler for Internett-tilgang ikke brytes?	5.7.4	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
206.	Blir pasienten/brukeren entydig identifisert ved elektronisk kommunikasjon?	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
207.	Er det etablert tekniske tiltak slik at all kommunikasjon med pasienten/brukeren krypteres iht gjeldende krav? Se. ”Kravspesifikasjon for PKI i offentlig sektor”.	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei
208.	Er løsningen slik at det ikke kan kommuniseres samtidig med andre parter enn den angitte pasient/bruker?	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt?	Sett inn referanse til dokumentasjon (om kravet er ivaretatt)	Kravet blir ivaretatt av databehandler
209.	Er løsningen slik at pasient/bruker ikke er avhengig av å lagre helse- og personopplysningene på eget utstyr for å gjøre seg kjent med informasjonen?	5.7.5	<input type="checkbox"/> Ja <input type="checkbox"/> Nei		<input type="checkbox"/> Ja <input type="checkbox"/> Nei