

 <p style="text-align: center;">Norm for informasjonssikkerhet www.normen.no</p>	<p>Utgitt med støtte av:</p>  HelseDirektoratet
<h2>Sikkerhetsrevisjon</h2> <h3>Sjekkliste for ivaretagelse av Normen</h3>	<p>Støttedokument Faktaark: 6b Versjon: 1.1 Dato: 15.12.2010</p>

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 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. Enkelte spørsmål kan være overlappende.

Kravet er referert til med kapittelnummer i Normen.

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
1.	Gjelder Normen for virksomheten? Normen er juridisk bindende for behandling av helse- og personopplysninger i alle virksomheter som er tilknyttet helsenettet eller som ved annen avtale har forpliktet seg til å følge Normen	1.6		
2.	Er det sendt melding/søkt om konsesjon til Datatilsynet for alle behandlinger av helse- og personopplysninger?	3.1 og 3.2.		
3.	Fornytes alle meldinger til Datatilsynet hvert 3. år?	3.1 og 3.2.		
4.	Er ledelsen klar over sitt ansvar som databehandlingsansvarlig?	3.1		
5.	Er ansvar og oppgaver for informasjonssikkerhet dokumentert i et organisasjonskart?	3.2		
6.	Er ansvar og oppgaver beskrevet på alle nivåer?	3.2		
7.	Er ansvarsforholdene gjort kjent i organisasjonen?	3.2		
8.	Er det etablert prosedyrer for bruk av papirutskrifter?	3.2		
9.	Er alle av sikkerhetstiltak dokumentert (organisatoriske, fysiske og tekniske)?	3.2		
10.	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		
11.	Arkiveres følgende 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 - Avtaler med partnere, databehandlere og leverandører 	3.3.4		
12.	Arkiveres hendelsesregistre med sikkerhetsmessig betydning, herunder registrering av autorisert bruk og forsøk på uautorisert bruk av informasjonssystemene, i minimum 2 år?	3.3.4		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
13.	Er det etablert et styringssystem for informasjonssikkerhet?	4.1		
14.	Er det fastsatt sikkerhetsmål for virksomheten?	4.2		
15.	Er formålene med behandlingene av helse- og personopplysninger dokumentert?	4.2.1		
16.	Er overordnede føringer for virksomhetens bruk av informasjonsteknologi dokumentert?	4.2.2		
17.	Er det utarbeidet sikkerhetsstrategi for å nå sikkerhetsmålene?	4.3		
18.	Er det dokumentert nivå for akseptabel risiko for konfidensialitet, tilgjengelighet, integritet og kvalitet?	4.4, 4.4.1, 4.4.2, 4.4.3, 4.4.4		
19.	Er det utarbeidet en samlet oversikt over alle behandlinger av helse- og personopplysninger i virksomheten?	4.5		
20.	Er det gjennomført og dokumentert risikovurderinger av alle behandlinger av helse- og personopplysninger? Risikovurdering skal som minimum gjennomføres 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	4.6		
21.	Er resultatet av risikovurderingene sammenlignet med fastlagt nivå for akseptabel risiko?	4.6		
22.	Er det etablert prosedyre for oppfølging av resultater fra risikovurderingene?	3.3.3		
23.	Er alle medarbeidere informert om sin taushetsplikt og klar over dens innhold og omfang?	5.1		
24.	Er konsekvenser ved brudd på taushetsplikten beskrevet?	5.1		
25.	Er konsekvenser ved å tilegne seg eller forsøke å tilegne seg opplysninger man ikke har tjenstlig behov for beskrevet?	5.1		
26.	Er konsekvenser ved å endre/forsøk på å endre opplysninger man ikke har autorisasjon til å endre beskrevet?	5.1		
27.	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		
28.	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		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
29.	Autoriseres bruker selvstendig for hver enkelt rolle?	5.2.1		
30.	Identifiseres brukeren i korrekt rolle i hvert enkelt tilfelle?	5.2.1		
31.	Identifiseres ulike ansettelsesforhold og er det ulike autentiseringskriteria ved behov?	5.2.1		
32.	Har alle personer unike autentiseringskriteria?	5.2.1		
33.	Gjennomføres tildeling av autentiseringskriteria (som brukernavn og passord) på en betryggende måte?	5.2.1		
34.	Benyttes sikkerhetsnivå 4 for autentisering ved bruk av mobilt utstyr, hjemmekontor og trådløs kommunikasjon?	5.2.1		
35.	Vurderes og ivaretas lovbestemt taushetsplikt ved tildeling av autorisasjon?	5.2.2		
36.	Har databehandlingsansvarlig delegert ansvar og myndighet for å tildele autorisasjon til den enkelte enhets ansvarlige leder?	5.2.2		
37.	Gis autorisasjon for å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger til dem som har tjenstlig behov?	5.2.2		
38.	Tildeles autorisasjonen i henhold til betryggende prosedyrer?	5.2.2		
39.	Registreres det i EPJ-systemet når autorisasjonen benyttes, med mindre risikovurdering avdekker at dette ikke er nødvendig.?	5.2.2		
40.	Autoriseres kun teknisk personell med særskilt behov for tilgang for større mengder helse- og personopplysninger?	5.2.2		
41.	Er det iverksatt tiltak slik at mulig misbruk kan avdekkes?	5.2.2		
42.	Tildeles autorisasjon for andre tjenester, f.eks. bruk av e-post og Internett, etter tjenstlig behov?	5.2.2		
43.	Er det bare autorisert personell som får tilgang til helse- og personopplysninger?	5.2.3		
44.	Gis tilgang etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten?	5.2.3		
45.	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		
46.	Ivaretas kravet i spørsmål 35. også i akutt situasjoner?	5.2.3		
47.	Fremgår det av journalen at tilgang i akutt situasjon er gitt der reglene om taushetsplikt krever det?	5.2.3		
48.	Utleveres eller gis helse- og personopplysninger til annet helsepersonell enn virksomhetens eget personell i samsvar med lovbestemte regler om taushetsplikt?	5.2.4		
49.	Behandles forespørsel om overføring, utlevering eller tilgang til helse- og personopplysninger i samsvar med betryggende prosedyrer?	5.2.4		
50.	Fremgår det av journalen når helse- og personopplysninger er gitt til annet helsepersonell enn virksomhetens eget personell?	5.2.4		
51.	Benyttes datasystemene bare til pålagte oppgaver?	5.2.5		
52.	Brukes datasystemene for privat brev/dokumentskrivning, utveksling av privat e-post m.m. i den grad dette ikke utsetter helse- og personopplysninger for risiko?	5.2.5		
53.	Registreres all autorisert bruk av informasjonssystemene?	5.2.6		
54.	Registreres alle forsøk på uautorisert bruk av informasjonssystemene?	5.2.6		
55.	Lagres registeret over autorisert og forsøk på uautorisert bruk i minimum 2 år?	5.2.6		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
56.	Gjennomføres det hendelsesregistrering av all tilgang der dette er nødvendig?	5.2.6		
57.	Kan hendelsesregistrene enkelt analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd?	5.2.6		
58.	Er det etablert prosedyrer for å analysere hendelsesregistrene slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke?	5.2.6		
59.	Iverksettes personalmessige reaksjoner dersom brudd avdekkes?	5.2.6		
60.	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.	5.2.6		
61.	Er hendelsesregistrene sikret mot endring og sletting av uautorisert personell?	5.2.6		
62.	Er det utarbeidet og iverksettes prosedyrer for behandling av helse- og personopplysninger?	5.3		
63.	Behandles brudd på prosedyrer som avvik?	5.3		
64.	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		
65.	Er det etablert prosedyre for nødrettstilgang?	5.3.1		
66.	Følges all bruk av nødrettstilgang opp som avvik?	5.3.1		
67.	Beskyttes autentiseringskriteria (bl.a. ved hemmeligholdelse av passord)?	5.3.1		
68.	Er alle helse- og personopplysninger som registreres relevante og nødvendige?	5.3.1		
69.	Registreres all informasjon snarest mulig etter at den har fremkommet?	5.3.1		
70.	Kontrolleres tilgangsstyring, herunder tildelte autorisasjoner, ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde?	5.3.2		
71.	Kontrolleres tilgangsstyring minimum årlig (gjærne i forbindelse med sikkerhetsrevisjon)?	5.3.2		
72.	Kontrolleres tilgangsstyring ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet?	5.3.2		
73.	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		
74.	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		
75.	Er pasienten sikret innsyn i egne helse- og personopplysninger?	5.3.3		
76.	Er pasientens rettigheter til retting/sletting av helse- og personopplysninger ivaretatt?	5.3.3		
77.	Er pasientens rett til sperring av hele eller deler av egen journal ivaretatt?	5.3.3		
78.	Er det etablert prosedyre for administrasjon av nøkler/adgangskort i adgangskontrollsystemet?	5.4.1		
79.	Er brukerstyr (arbeidsstasjon, PC og skrivere) sikret slik at personer som ikke er autoriserte ikke får tilgang til helse- og personopplysninger?	5.4.2		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
80.	Er det etablert sikkerhetstiltak slik at kun autorisert personell får adgang til driftsutstyr (servere og nettverksutstyr)?	5.4.3		
81.	Er det gjennomført risikovurdering av mobilt utstyr og hjemmekontor?	5.4.4		
82.	Er det etablert administrative prosedyrer for bruk av mobilt utstyr og hjemmekontor?	5.4.4		
83.	Er det iverksatt tekniske tiltak slik at mobilt utstyr og hjemmekontor kun kan kommuniseres med predefinert utstyr?	5.4.4		
84.	Er helse- og personopplysninger som lagres lokalt på mobilt utstyr og hjemmekontor kryptert iht gjeldende krav?	5.4.4		
85.	Er all kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer kryptert iht gjeldende krav?	5.4.4		
86.	Er lagringsenhet for medisinsk teknisk utstyr som behandler helse- og personopplysninger plassert i avlåst rom eller i bemannet område?	5.4.5		
87.	Er medisinsk teknisk 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		
88.	Har virksomheten oversikt over og kontroll på alt utstyr og programvare som benyttes i behandlingen av helse- og personopplysninger?	5.5.1		
89.	Utfører konfigurasjonen av utstyret og programvaren kun de funksjoner som er formålsbestemt?	5.5.1		
90.	Settes konfigurasjonsendringer, dvs. endringer i utstyr og/eller programvare, først i drift når følgende tiltak er gjennomført? - 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		
91.	Er det iversatt minst to uavhengige tekniske tiltak slik at personer utenfor virksomheten uansett ressurser og kunnskap ikke skal kunne få tilgang til og/eller kunne endre eller slette helse- og personopplysninger?	5.5.2		
92.	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		
93.	Er det etablert tekniske tiltak slik at helsepersonell i nødrettssituasjoner, kan få tilgang til nødvendige helse- og personopplysninger (nødrettstilgang)?	5.5.2		
94.	Grunngis og registreres bruk av nødrettstilgang i EPJ-systemet?	5.5.2		
95.	Behandles bruk av nødrettstilgang som avvik?	5.5.2		
96.	Er det etablert tekniske tiltak slik at personer innenfor virksomheten uansett ressurser og kunnskap ikke skal kunne endre opplysninger uten at det registreres i EPJ-systemet hvem som har endret og hva som er endret?	5.5.2		
97.	Er det iverksatt to uavhengige tekniske tiltak slik at uautorisert programvare ikke skal kunne endre helse- og personopplysninger?	5.5.2		
98.	Skiller systemet som administrerer autorisasjon mellom rettigheter til å lese, registrere, redigere, rette, slette og/eller sperre helse- og personopplysninger?	5.5.2		
99.	Registreres all tildeling av autorisasjon i systemet som administrerer autorisasjon?	5.5.2		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
100.	Har alle systemer mekanismer som hindrer uautoriserte endringer av helse- og personopplysninger?	5.5.2		
101.	Er tilgang fra avdelingskontor, hjemmekontor og/eller mobilt utstyr, som kommuniserer ved hjelp av linjer man ikke har fysisk kontroll over, sikret med sikkerhetsnivå 4 for autentisering?	5.5.2		
102.	Er alle lagringsmedia, dvs. disketter, CD-ROM mv., merket?	5.5.2		
103.	Slettes alle helse- og personopplysninger når lagringsmediet tas ut av bruk?	5.5.2		
104.	Overholdes plikten til arkivering av opplysningene når lagringsmediet tas ut av bruk?	5.5.2		
105.	Hendelsesregistreres autorisert bruk av informasjonssystemene?	5.5.2		
106.	Hendelsesregistreres sikkerhetsrelevante hendelser i sikkerhetsbarrierene, bl.a. forsøk på uautorisert bruk av informasjonssystemet?	5.5.2		
107.	Hendelsesregistreres alle forsøk på uautorisert bruk av nettverksoperativsystemer?	5.5.2		
108.	Hendelsesregistreres alle forsøk på uautorisert bruk av alle informasjonssystemer?	5.5.2		
109.	Hendelsesregistreres bruk av nødrettstilgang?	5.5.2		
110.	Har virksomheten etablert nødprosedyrer for alternativ drift uten bruk av informasjonssystemene?	5.5.3		
111.	Har virksomheten etablert nødprosedyrer for alternativ drift med delvis støtte fra informasjonssystemene?	5.5.3		
112.	Testes prosedyrene for alternativ drift minimum årlig?	5.5.3		
113.	Har virksomhetens ledelse sørget for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk?	5.5.3		
114.	Oppbevares sikkerhetskopier avlåst og brannsikret, og adskilt fra driftsutstyret?	5.5.3		
115.	Foretas det jevnlig test at sikkerhetskopiene er korrekte og kan tilbakeføres?	5.5.3		
116.	Har virksomheten fastsatt prosedyrer for å ivareta kravene til kvalitet?	5.5.4		
117.	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		
118.	Er det, ved tilkobling til nett utenfor virksomheten, etablert tekniske tiltak som ivaretar at kun eksplisitt angitt tillatt trafikk kan passere, annet stoppes?	5.7.1		
119.	Er det, ved tilkobling til nett utenfor virksomheten, etablert tekniske tiltak som ivaretar at trafikk ikke kan passere direkte utenfra og inn; all slik ekstern trafikk må initieres fra virksomhetens systemer?	5.7.1		
120.	Er det, ved tilkobling til nett utenfor virksomheten, etablert tekniske tiltak som ivaretar hendelsesregistrering for å kontrollere at regler ikke brytes; ved brudd stenges kanalen inntil ny sikker løsning finnes?	5.7.1		
121.	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		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
122.	Er det avtalt at avsender er ansvarlig for: <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		
123.	Er det avtalt at mottaker er ansvarlig for: <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		
124.	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		
125.	Har virksomheten iverksatt tiltak for å forhindre at sensitive personopplysninger utleveres ved hjelp av e-post?	5.7.3		
126.	Har virksomheten forsikret seg om ved tekniske tiltak og organisatoriske tiltak at e-post ikke inneholder sensitive personopplysninger?	5.7.3		
127.	Er det iverksatt hendelsesregistrering for bruk av e-post for å kontrollere at regler ikke brytes?	5.7.3		
128.	Behandles regelbrudd ved sending av e-post med sensitive personopplysninger som avvik?	5.7.3		
129.	Vurderes personalmessige konsekvenser ved sending av e-post med sensitive personopplysninger?	5.7.3		
130.	Er det iverksatt tekniske tiltak som sikrer at Internett-tjenesten er logisk atskilt fra der helse- og personopplysninger behandles?	5.7.4		
131.	Er det iverksatt hendelsesregistrering for å kontrollere at regler for Internett-tilgang ikke brytes?	5.7.4		
132.	Behandles regelbrudd ved bruk av Internett som avvik?	5.7.4		
133.	Vurderes det personalmessige konsekvenser ved brudd på bruk av Internett?	5.7.4		
134.	Er det innhentet samtykke fra pasienten/brukeren for å formidle helse- og personopplysninger elektronisk?	5.7.5		
135.	Blir pasienten/brukeren entydig identifisert ved elektronisk kommunikasjon?	5.7.5		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
136.	Er det etablert tekniske tiltak slik at all kommunikasjon med pasienten/brukeren krypteres iht gjeldende krav?	5.7.5		
137.	Er løsningen slik at det ikke kan kommuniseres samtidig med andre parter enn den angitte pasient/bruker?	5.7.5		
138.	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		
139.	Er det inngått avtale med kommunikasjonsleverandør iht kravene i Normen? Norsk Helsenett er en kommunikasjonsleverandør. <i>Benyttes ikke kommunikasjonsleverandør kan svaret IR = Ikke relevant angis.</i>	5.8.1		
140.	Er det inngått avtale med databehandler iht kravene i Normen? <i>Benyttes ikke databehandler kan svaret IR = Ikke relevant angis.</i>	5.8.2		
141.	Har databehandler gjennomført risikovurdering, ved etablering av skille mellom flere virksomheter, når databehandler er databehandler for flere virksomheter? <i>Benyttes ikke databehandler kan svaret IR = Ikke relevant angis.</i>	5.8.2		
142.	Er det inngått avtale med leverandør iht kravene i Normen? <i>Benyttes ikke leverandør kan svaret IR = Ikke relevant angis.</i>	5.8.3		
143.	Er det inngått avtale med sikkerhetsleverandør iht kravene i Normen? <i>Benyttes ikke sikkerhetsleverandør kan svaret IR = Ikke relevant angis.</i>	5.8.4		
144.	Gjennomføres det sikkerhetsrevisjon minimum årlig?	6.1		
145.	Foreligger det en plan for sikkerhetsrevisjoner?	6.1		
146.	Dekker sikkerhetsrevisjonen minimum?: - 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		
147.	Dokumenteres resultatet av sikkerhetsrevisjonene?	6.1		
148.	Er det etablert prosedyre for oppfølging av resultatet av sikkerhetsrevisjoner?	3.3.3		
149.	Behandles bruk av informasjonssystemene som ikke er forutsatt som avvik?	6.1		
150.	Er det etablert prosedyre for behandling av avvik?	6.3		
151.	Er alle medarbeidere klar over ansvaret de har for å melde avvik?	6.3		
152.	Rapporteres behandling av avvik til ledelsen i virksomheten?	6.3		
153.	Er det etablert prosedyre som sikrer at Datatilsynet varsles ved uautorisert utlevering av helse- og personopplysninger?	6.3		
154.	Gjennomføres det ledelsens gjennomgang minimum årlig?	6.4		

Nr	Krav	Kapittel i Normen	Er kravet ivaretatt	
			Ja	Nei
155.	Dekker ledelsens gjennomgang minimum?: - 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	6.4		
156.	Vedtas det tiltaksplaner dersom ledelsens gjennomgang avdekker at virkelig situasjon ikke når opp til fastsatt nivå for akseptabel risiko?	6.4		
157.	Er det etablert prosedyre for oppfølging av handlingsplaner besluttet av ledelsen?	3.3.3		