

Aktøroversikt: Spesialisthelsetjenesten i en region er alvorlig rammet av digital skadevare

Utgave: 24. oktober 2025

Introduksjon

Hensikten med denne aktøroversikten er å gi en oversikt over aktørbildet ved en alvorlig digital hendelse i helse- og omsorgssektoren. Aktørbildet er komplekst, og denne aktøroversikten er et eksempel på hvordan aktørbildet kan se ut. Aktøroversikten kan brukes som en ressurs inn i arbeidet med å forberede seg på å håndtere alvorlige digitale hendelser i helse- og omsorgssektoren, på nasjonalt nivå, på regionalt nivå og i den enkelte virksomhet.

Aktøroversikten er laget basert på et scenario hvor spesialisthelsetjenesten i en region er alvorlig rammet av skadevare. Dersom man ser for seg et annet scenario, vil aktøroversikten endres tilsvarende. Aktøroversikten er under utarbeidelse, og vi ønsker gjerne tilbakemeldinger på innholdet i den.

Scenario

Aktøroversikten er laget med utgangspunkt i følgende scenario:

Skadevare har fått fotfeste i en region

- Flere sykehus er rammet, gjenoppretting er vanskelig på kort sikt
- Systemer som er rammet:
 - Journalsystemet, labsystem, sykehusapotek
 - Tilgangsstyringssystem til bygg
- Hendelsen ble oppdaget i dag
- Har konsekvenser for behandling av pasienter
 - Elektiv behandling må utsettes
 - En del pågående behandlingsløp må avbrytes
- Kan ikke motta elektroniske henvisninger
- Aktiv bistand fra HelseCERT
 - Mangler foreløpig oversikt over omfang av hendelsen og hva som egentlig har skjedd
- Media skriver om hendelsen, og det er uro og usikkerhet i befolkningen i området som er berørt

I aktøroversikten er det antatt at kommunehelsetjenesten og spesialisthelsetjenesten ikke har felles journalsystem.

Metodikk

Aktøroversikten er under utarbeidelse, og dette er en foreløpig versjon. Det oppfordres til å komme med tilbakemeldinger på aktøroversikten, for eksempel dersom det oppdages unøyaktigheter eller feil, eller det er aspekter som man synes mangler. Ta i så fall kontakt på e-post til sekretariatet for utvalg digital sikkerhet og beredskap ved Knut Herje (knut.herje@helsedir.no).

Aktøroversikten er laget med utgangspunkt i:

- Flere gruppearbeid i utvalg for digital sikkerhet og beredskap
- Nasjonal helseberedskapsplan (<https://www.regjeringen.no/no/dokumenter/nasjonal-helseberedskapsplan/id3102492/>)
- Nasjonalt rammeverk for digitale angrep og cyberhendelser (<https://nsm.no/regelverk-og-hjelp/rapporter/nasjonalt-rammeverk-for-handtering-av-digitale-angrep-og-cyberhendelser>)

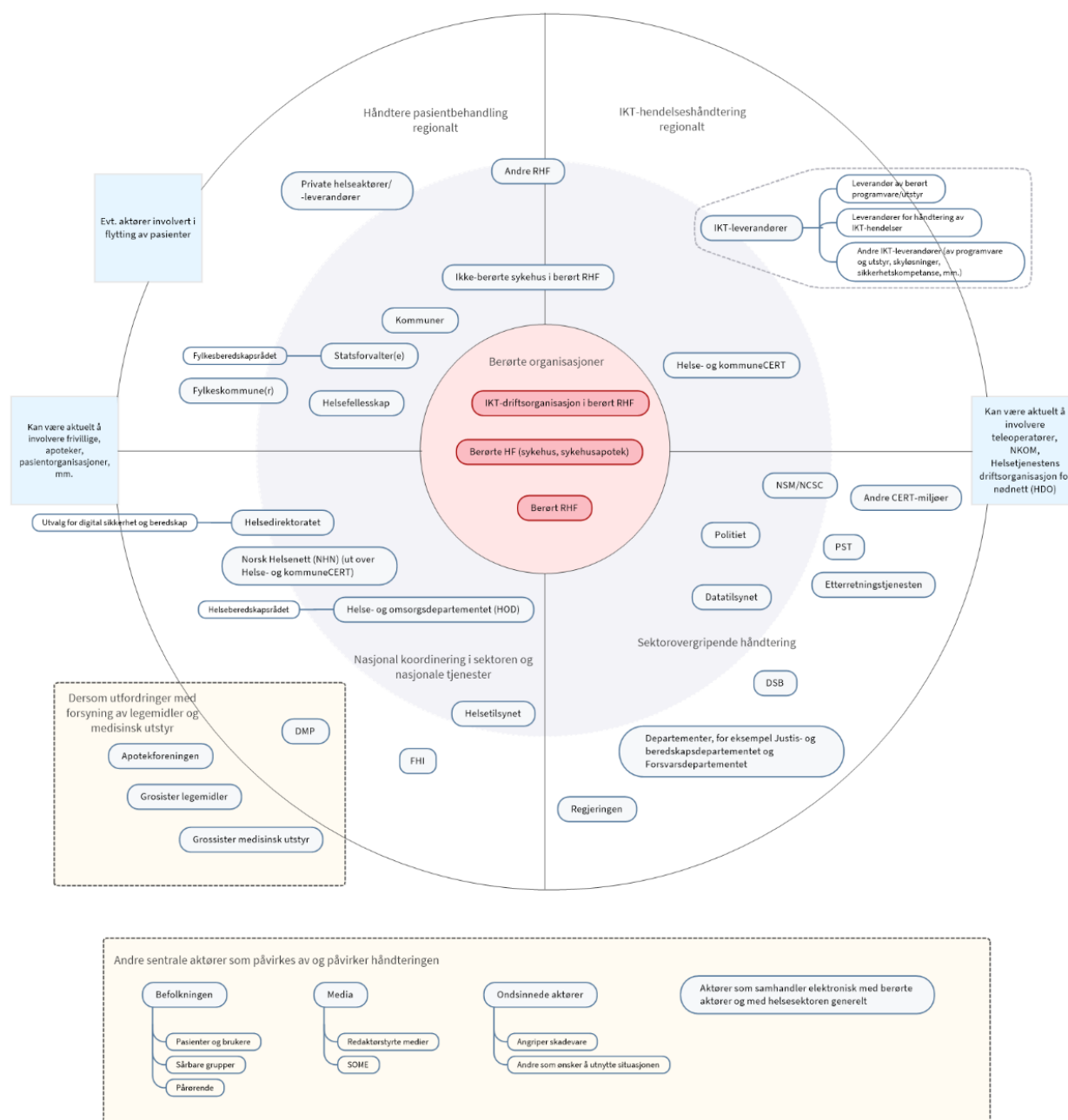
Nasjonal helseberedskapsplan er det overordnede rammeverket som dekker alle typer hendelser innen helse- og omsorgssektoren. Nasjonalt rammeverk for digitale angrep og cyberhendelser beskriver samarbeidet mellom virksomheter, sektorvise responsmiljøer (slik som Helse- og kommuneCERT) og Nasjonalt cybersikkerhetssenter (NCSC) ved digitale angrep og cyberhendelser. Disse to rammeverkene må ses i sammenheng, og aktøroversikten bidrar til dette ved å benytte begge som underlag. I beskrivelsene av aktørene, og deres ansvar og samhandlingsparter, er rapporteringsveiene i både Nasjonal helseberedskapsplan og Nasjonalt rammeverk for digitale angrep og cyberhendelser lagt til grunn. For en full forståelse av og oversikt over innholdet i disse rammeverkene er det imidlertid nødvendig å se til de fullstendige beskrivelsene i Nasjonal helseberedskapsplan og i Nasjonalt rammeverk for digitale angrep og cyberhendelser.

Innspill til aktøroversikten, gjennom tilbakemeldinger og gjennom videre arbeid i utvalg for digital sikkerhet og beredskap, vil gi grunnlag for oppdateringer av aktøroversikten.

Aktøroversikt

Aktøroversikten gir en oversikt over aktørene som er eller kan være involvert i håndteringen av en hendelse av den type som er beskrevet i scenariet som er utgangspunkt for aktøroversikten. Aktøroversikten er et eksempel og gir en oversikt over hvilke aktører som kan være involvert, ikke en beskrivelse av hvordan det bør være.

For å gi en oversikt, så er aktørene plassert i ulike aktørgrupper. Inndelingen av aktører, f.eks. i de som håndterer konsekvenser for pasientbehandling og de som bidrar inn i IKT-hendelseshåndtering, betyr **ikke** betyr at dette ses som to separate håndteringsspor – det er svært viktig at håndtering av hendelsen har søkelys på begge disse aspektene og ser de i sammenheng. Håndtering av hendelsen innebærer at man håndterer "hele sirkelen".



Aktøroversikten i figuren under er bygd opp slik:

- *Berørte organisasjoner:* De organisasjonene som er direkte berørt er vist i midten av kartet, og er gitt en egen farge (rød). Hvilke aktører som plasseres i rollen "berørt organisasjon" er svært avhengig av scenariet og er et eksempel. Som eksempel, dersom scenariet i stedet antar at kommunehelsetjenesten og spesialisthelsetjenesten deler journalsystem, så vil alle sykehus i regionen samt kommuner også være berørte organisasjoner.
- Andre aktører er delt inn i aktører som har roller på følgende områder:
 - *Håndtere pasientbehandling regionalt:* Bidra til at utfordringer knyttet til pasientbehandlingen håndteres, for eksempel ved å bistå berørte sykehus og ved å håndtere eventuelle konsekvenser for pasientbehandling som spres til andre aktører (slik som kommuner).
 - *IKT-hendelseshåndtering regionalt:* Bidra til å håndtere IKT-biten av hendelseshåndteringen, noe som inkluderer å vurdere og klassifisere hendelsen og å kontrollere og håndtere hendelsen.
 - *Nasjonal koordinering i sektoren og nasjonale tjenester:* Innebærer vurderinger og eventuelle tiltak på nasjonalt nivå i helse- og omsorgssektoren, inkludert vurderinger og tiltak knyttet til nasjonale tjenester.
 - *Sektorovergripende håndtering:* Inkluderer aktører som har roller i håndteringen, men som ikke regnes som en del av helse- og omsorgssektoren, slik som politiet, NSM og Datatilsynet.
- Aktører som involveres mye og tidlig er plassert nærmere sentrum i ringen. Aktører som det er mer usikkert om hvor mye vil involveres i tidlig fase i dette scenarioet er plassert lenger ut.
- Noen aktørtyper har ikke fått plass i "ringen" i aktøroversikten, men nevnes i egen boks under. Dette gjelder aktører som påvirker og/eller påvirkes av hendelsen og håndteringen, men som ikke hører direkte til i ett av de fire områdene og som ikke har direkte ansvar i hendelseshåndteringen.

I underkapitlene som følger er de ulike typene av aktører beskrevet i mer detalj, med fokus på hvilken rolle de har (aksjoner, ansvar) og hvem de samhandler med. I de tilfeller der en aktør er del av flere områder (for eksempel ikke-berørte sykehus som både har en rolle i å håndtere pasientkonsekvenser og IKT-biten av hendelsen) så er aktøren beskrevet under begge områdene.

Berørte organisasjoner

I dette scenarioet er følgende organisasjoner direkte berørt av hendelsen:

- Flere sykehus og sykehusapotek i en region
- IKT-driftsorganisasjonen i berørt region
- Det regionale helseforetaket (RHF)

Hvordan disse organisasjonene har valgt å organisere koordinering og ansvarsforhold seg imellom vil kunne variere mellom regioner, men i all hovedsak kan man forvente følgende:

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
Berørt RHF	• Koordinere håndteringen i regionen og bidra til at spesialisthelsetjenestens krisehåndtering er koordinert med kommunene i regionen • Varsle sentrale myndigheter og informere statsforvalter (koordinert med berørte HF) • Koordinere eventuelle henvendelser om bistand fra egen region • Koordinere mediehåndtering i regionen • Håndtere innsynskrav (koordinere med andre relevante aktører)	• HF (berørte og ikke-berørte) i regionen • IKT-driftsorganisasjon i regionen • HOD • Statsforvalter(e) • Andre RHF Ved behov: • Kommuner • Helsedirektoratet • DMP • Helsetilsynet
Berørte sykehus (HF)	• Varsle RHF og IKT-driftsorganisasjon • Anmelde til politiet • Vurdere alvorlighetsgrad, omfang og konsekvenser av hendelsen • Håndtere konsekvenser for pasientbehandlingen (f.eks. ved å avlyse behandling, mobilisere ressurser, flytte pasienter) – når relevant, i samarbeid med kommuner, statsforvalter og andre HF • Håndtere risiko og digitale hendelser evt. digitale systemer hvor man har ansvar for drift selv • Varsle Datatilsynet • Sende melding til Helsetilsynet • Kan kommunisere helsekonsekvenser med media (koordinert med RHF) • Håndtere innsynskrav (koordinere med andre relevante aktører)	• RHF • IKT-driftsorganisasjon • Statsforvalter • Kommuner • Andre HF i regionen • Politi • Datatilsynet • Helse- og kommuneCERT • Helsetilsynet Ved behov: • Helsedirektoratet • Norsk helsenett • DMP • FHI • Frivillige
Berørt sykehusapotek (HF)	• Varsle RHF og IKT-driftsorganisasjon • Anmelde til politiet • Vurdere alvorlighetsgrad, omfang og konsekvenser av hendelsen • Håndtere konsekvenser for driften av apotek tjenester	• RHF • IKT-driftsorganisasjon • HF i regionen • Politi • Datatilsynet • Helse- og kommuneCERT • DMP

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
	• Håndtere risiko og digitale hendelser evt. digitale systemer hvor man har ansvar for drift selv • Varsle Datatilsynet • Sende melding til Helsetilsynet • Kan kommunisere om konsekvenser til media (koordinert med RHF) • Håndtere innsynskrav (koordinere med andre relevante aktører)	• Helsetilsynet Ved behov: • Apotekforeningen • Grossister legemidler
IKT-drifts-organisasjon (HF/AS) (inkl. evt. intern CERT)	• Varsle RHF og berørt HF dersom det er de som oppdager hendelsen, og gi statusoppdateringer og råd undervegs • Vurdere alvorlighetsgrad, omfang og konsekvenser av hendelsen • Snarest vurdere behov for støtte eller bistand, samt hente inn nødvendig bistand fra HelseCERT og leverandører • Håndtere IKT-delen av hendelsen med mål om å redusere konsekvensene av hendelsen og gjenopprette sikker tilstand – inkludert iverksette sikkerhetstiltak i egen region for å hindre spredning • Ha/få nødvendige fullmakter • Samarbeide med politi • Varsle NSM dersom skjermingsverdig objekt/infrastruktur er rammet, og håndtere videre samarbeid (inkl. gradering) • Kan kommunisere om IKT-delen av hendelsen til media (koordinert med RHF) • Håndtere innsynskrav (koordinere med andre relevante aktører)	• RHF • HF i regionen – både berørte og ikke-berørte • Helse- og kommuneCERT • IKT-leverandører • Politi • NSM Ved behov: • IKT-driftsorganisasjoner i andre regioner • Norsk helsenett • Helsedirektoratet (reseptformidleren, kjernejournal)

Håndtere pasientbehandling regionalt

Konsekvenser for pasientbehandling håndteres primært av berørt RHF og HF, i samhandling med andre viktige aktører slik som kommuner og statsforvalter. Det kan søkes bistand fra andre HF og fra private aktører.

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
Ikke-berørte sykehus i berørt RHF	• Dialog og koordinering med RHF og andre HF i regionen • Kan bidra ved å f.eks. ta imot pasienter fra berørte sykehus	• Berørt RHF • Berørte HF og andre HF i regionen Ved behov: • Kommuner • Statsforvalter
Kommuner	• Motta informasjon om hendelsen fra spesialisthelsetjenesten • Håndtere følgekonsekvenser (f.eks. økt mengde henvendelser), koordinert med spesialisthelsetjenesten: Legevakt, fastleger, sykehjem, hjemmetjenester, mv. • Gi informasjon, råd og veiledning til innbyggerne i kommunen (budskap koordinert med spesialisthelsetjenesten og evt. nasjonale myndigheter) • Rapportere til statsforvalter • Be om bistand fra statsforvalter og andre kommuner og instanser ved behov	• Berørt HF • Statsforvalter • Helsefelleskap Ved behov: • Andre kommuner • KS • Berørt RHF
Statsforvalter(e)	• Motta informasjon fra spesialisthelsetjenesten om hendelsen • Varsle Helsedirektoratet • Sendte melding til Helsetilsynet • Skaffe oversikt over situasjonen i fylket • Rapportere til Helsedirektoratet og Direktoratet for samfunnssikkerhet og beredskap • Bidra til samordning i den regionale krisehåndteringen og være et bindeledd mellom lokalt og nasjonalt nivå, f.eks. ved å avklare spørsmål fra kommunene, koordinere tiltak og informasjon med RHF, samordne mot andre fylker, kartlegge behov i kommunene og ta initiativ mot sentrale myndigheter ang. ressursbehov.	• Berørt RHF • Berørt(e) HF • Relevante kommuner • Relevant(e) fylkeskommune(r) • Helsedirektoratet • Direktoratet for samfunnssikkerhet og beredskap • Fylkesberedskapsrådet

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
	• Kan samle Fylkesberedskapsrådet • Forberede ressurser som statsforvalter kan mobilisere, f.eks. Fylkeskommunens transportberedskap	
Helsefellesskap	• Samarbeidsarena mellom spesialisthelsetjenesten og kommuner • Evt. benytte deres administrative beredskapsutvalg der dette finnes	• HF • Kommuner
Fylkeskommune(r)	• Motta informasjon om hendelsen fra statsforvalter, evt. fra spesialisthelsetjenesten • Håndtere følgekonskvenser, f.eks. for tannhelsetjenesten og transportberedskap	• Statsforvalter Ved behov: • HF • RHF • Kommuner
Fylkesberedskapsrådet	• Mulig forum for å ivareta samordning i håndtering av hendelsen	• Rådets medlemmer
Andre RHF	• Evt. bistå berørt region etter forespørsel • Gjøre egne forberedelser basert på risikosituasjonen	• Berørt RHF Ved behov: • HOD • Statsforvaltere • Helsedirektoratet
Private helseaktører/-leverandører	• Kan involveres av berørt RHF/HF ved behov for tjenester	• Berørt RHF • Berørt HF

IKT-hendelseshåndtering regionalt

IKT-hendelseshåndtering gjøres primært av **IKT-driftsorganisasjon i berørt region**, men det er naturlig å søke bistand hos andre aktører (se tabell under). Dersom **berørte HF** (sykehus og sykehusapotek) har ansvar for drift av noen av sine egne IKT-systemer, så vil de også ha ansvar for risiko- og hendelseshåndtering når det gjelder disse systemene, men kan søke bistand. Håndtering av IKT-delen av hendelsen må ikke ses isolert fra håndtering av konsekvenser for pasientbehandlingen.

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
Helse- og kommuneCERT	• Bistå berørt virksomhet i hendelseshåndteringen • Ha oversikt over omfanget av cyberhendelsen på sektornivå, se angrep på ulike virksomheter i sammenheng og koordinere den digitale hendelseshåndteringen i sektoren • Tidsriktig varsle NCSC, relevante SRM og virksomheter • Varsle relevante myndigheter om alvorlig hendelse • Dele relevant informasjon innen egen sektor og gi råd til virksomheter i sektoren • I samarbeid med virksomheter i sektoren, gjøre tiltak for å kartlegge og avdekke digitale angrep • Holde NCSC løpende orientert om utviklingen i hendelsesforløpet	• Berørte virksomheter, og spesielt IKT-driftsorganisasjon til berørt virksomhet • NCSC • Andre SRM/CERT-miljøer • Virksomheter i sektoren som ikke er berørt, spesielt IKT-driftsorganisasjoner i andre regioner • HOD • NHN (ut over HelseCERT)
Ikke-berørte sykehus i berørt RHF	• Motta og vurdere informasjon fra IKT-driftsorganisasjon, berørte HF, RHF og HelseCERT, oppdatere risikobilde for egne systemer • Iverksette sikkerhetstiltak for å hindre spredning og minimere eventuelle konsekvenser	• IKT-driftsorganisasjon • Helse- og kommuneCERT • Berørte HF • RHF
Andre RHF (primært IKT-driftsorganisasjon)	• Oppdatert risikobilde • Gjøre risikoreduserende tiltak • Kan bistå berørt region ved forespørsel	• IKT-driftsorganisasjon i berørt region • Helse- og kommuneCERT
Leverandør av berørt programvare/utstyr	• Kan involveres ved behov • Iverksette sikkerhetstiltak	• IKT-driftsorganisasjon • Berørt HF
Leverandører for håndtering av IKT-hendelser	• Kan involveres ved behov	• IKT-driftsorganisasjon • Berørt HF
Andre IKT-leverandører	• Kan involveres ved behov • Kan ønske distanse for å unngå spredning av skadevare	• IKT-driftsorganisasjon

Nasjonal koordinering i sektoren og nasjonale tjenester

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
Helse- og omsorgsdepartementet (HOD)	- Varsles om hendelsen fra berørte underliggende virksomheter - Være orientert om hendelsen og håndteringen - Har ansvar for tiltak i sektoren i krisesituasjoner og har fullmakter til å iverksette nødvendige tiltak i en krise - Vil avklare egen rolle i håndteringen av større ekstraordinære hendelser, og evt. beslutte nasjonal koordinering. Kan da delegere oppgaver til Helsedirektoratet eller andre, og vil da kommunisere dette til alle berørte - Påse at operative aktører har nødvendige fullmakter - Kan instruere virksomheter departementet har instruksjonsmyndighet over - Koordinere seg med andre departementer, f.eks. Justis- og beredskapsdepartementet - Rapportere til regjeringen	- Berørt RHF - Andre RHF - Norsk helsenett - Helsedirektoratet - Regjering, departementer Ved behov: - DMP - FHI
Norsk helsenett (NHN) (ut over Helse- og kommuneCERT)	- Drift av nasjonale tjenester, inkludert stamnett - Oppdatert risikoforståelse, og tilhørende risikoreduserendetiltak for tjenester de har ansvar for - Beslutninger knyttet til utestenging, isolering og nedstenging o.l. tas sammen med relevante aktører (eks. HOD, Helsedirektoratet)	- HOD - Helsedirektoratet (dersom det gjelder Kjernejournal eller reseptformidleren) Ved behov: - RHF – berørte og andre - HF – berørte og andre - Leverandører
Helse- direktoratet	- Oppdatert risikoforståelse og risikoreduserendetiltak knyttet til systemer de har ansvar for, inkl. kjernejournal og reseptformidleren - Beslutninger knyttet til utestenging, isolering og nedstenging o.l. av kjernejournal og reseptformidleren tas sammen med relevante aktører (eks. HOD, NHN) - Motta varsel fra statsforvalter, og kan motta oppdateringer fra RHF, NHN, HOD, mm. - Kontakt mot statsforvaltere	- Statsforvaltere - NHN - HOD Ved behov: - Utvalg for digital sikkerhet og beredskap - Berørt RHF - Berørt HF - Apotek - DMP - Kommuner

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
	• Kan få oppgaver fra HOD, bl.a. knyttet til felles situasjonsforståelse, kommunikasjon og innhenting av informasjon om status og resultater av tiltak • På forespørsel: Juridiske avklaringer, støtte til prioriteringer • Kan involvere utvalg for digital sikkerhet og beredskap	
Utvalg for digital sikkerhet og beredskap	• Kan, ved behov og om hensiktsmessig, samles for felles situasjonsforståelse, diskusjon og samordning av tiltak, o.l.	• Helsedirektoratet • Utvalgets medlemmer
Helseberedskapsrådet	• Kan benyttes av HOD for å utarbeide felles situasjonsforståelse og legge til rette for hurtig og koordinert iverksettelse av tiltak	• HOD • Rådets medlemmer
Direktoratet for medisinske produkter (DMP)	• Bistå med å håndtere eventuelle utfordringer knyttet til forsyning av legemidler og medisinsk utstyr	• Apotekforeningen • Grossister Ved behov: • Berørt RHF • Berørte HF
Folkehelseinstituttet (FHI)	• Håndtere risiko knyttet til nasjonale register de har ansvar for – oppdatert risikobilde og risikoreduserende tiltak	• HOD
Helsetilsynet	• Motta melding om hendelsen • Vurdere videre tilsynsmessig oppfølging	• Berørte HF • Statsforvaltere
Apotekforeningen	• Koordinerer landets apotek	• DMP • Apoteker, inkl. sykehusapotek
Grossister legemidler	• Kan involveres ved mangel eller risiko for mangel på legemidler	• DMP • Berørt sykehusapotek Ved behov: • Apotekforeningen
Grossister medisinsk utstyr	• Kan involveres ved behov for medisinsk utstyr	• DMP • Berørt HF, evt. IKT-driftsorganisasjon i berørt region

Sektorovergripende håndtering

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
NSM/NCSC (Nasjonal Sikkerhetsmyndighet / Nasjonalt cybersikkerhetsse- nter)	NSM: - Vurdere om kritiske samfunnsfunksjoner og/eller grunnleggende nasjonale funksjoner er eller står i fare for å bli berørt av digitalt angrep - Har kvalitetsordning for leverandører som håndterer IKT-hendelser NCSC: - Ivareta rollen som nasjonal varslings- og koordineringsinstans for digitale angrep - Etablere situasjonsforståelse ved å ha oversikt over relevante risikoer og hendelser på tvers av sektorer og land - Gi råd og veiledning til SRM og virksomheter i forbindelse med hendelseshåndteringen - Kan, ved alvorlige angrep, bistå på teknisk nivå i hendelseshåndteringen - Ved alvorlige digitale angrep kan NCSC koordinere nasjonal hendelseshåndtering og anbefale tiltak til politisk ledelse	- Helse- og kommuneCERT - Andre SRM - IKT-driftsorganisasjon i berørt RHF - Berørte HF - Internasjonale samarbeidspartnere - Felles cyber-koordineringssenter (FCKS) Ved behov: - Berørte RHF - Andre relevante virksomheter med ansvar for GNF - Justis- og beredskapsdepartementet - Forsvarsdepartementet - NCSC-partnervirksomheter
Politiet	- Motta anmeldelse - Sikre tekniske spor, gjøre beslag, etterforskning og pågripelser	- Berørt HF - IKT-driftsorganisasjon i berørt region - Felles cyber-koordineringssenter (FCKS) - PST
Politiets sikkerhetstjeneste (PST)	Innhente informasjon om personer og grupper som kan utgjøre en trussel	- Politiet - Felles cyber-koordineringssenter (FCKS) - Etterretnings-tjenesten
Etterretnings-tjenesten	Innhente informasjon om utenlandske aktører som kan utgjøre en trussel	- Felles cyber-koordineringssenter (FCKS) - PST
Datatilsynet	Varsles ved hendelser som gir personvernkonsekvenser	Berørt HF

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
Andre CERT-miljøer	Informasjons- og erfaringsutveksling (nasjonalt og internasjonalt)	- Helse- og kommuneCERT - NCSC
DSB (Direktoratet for samfunnssikkerhet og beredskap)	- Skal ha oversikt over risiko og sårbarhet i samfunnet - Skal sørge for god beredskap og effektiv krisehåndtering	- Statsforvalter - Helsedirektoratet - Justis- og beredskapsdepartementet
Departementer, f.eks. Justis- og beredskapsdepartementet og Forsvarsdepartementet	- Justis- og beredskapsdepartementet er fast lederdepartement i sivile nasjonale kriser, og har samordningsansvar for digital sikkerhet i sivil sektor - NSM og DSB ligger under Justis- og beredskapsdepartementet. NSM jobber også med digital sikkerhet innen Forsvarsdepartementets ansvarsområde	- HOD - NSM - DSB
Regjeringen	- Har det øverste ansvaret for nasjonal sikkerhet og beredskap - Kongen i statsråd kan utløse fullmaktsbestemmelsene i helseberedskapsloven	HOD og andre departementer

Andre sentrale aktører som påvirkes av og påvirker håndteringen

Aktør	Aksjoner og ansvar	Viktige samhandlingsparter
Befolkning	Trenger informasjon om situasjonen og hvordan de skal forholde seg	- Media - Berørt HF - Berørt RHF - Kommuner Ved behov: - Helsedirektoratet - HOD
Media	- Kan be om oppdateringer om situasjonen - Mulig kanal for å få ut budskap til befolkningen, f.eks. om hvordan forholde seg til timeavtaler på berørte sykehus - Kan fremme innsynskrav	- Berørte HF - Berørt RHF - HOD - Kommuner Ved behov: - Helsedirektoratet
Ondsinnede aktører	- Angrep, fremme krav, eskalere - Kan fremme innsynskrav	
Aktører som samhandler elektronisk med berørte aktører og med helsesektoren	Kan velge å unngå samhandling, evt. koble seg fra, for å unngå å bli utsatt for skadevare	