Veileder i digital pasientkommunikasjon for helse- og omsorgssektoren

Versjon 3.0

2. februar2020

Utgitt med støtte av:

Direktoratet for e-helse

Endringshistorikk for og godkjenning av dokumentet

Versjon	Endringer	Godkjent av styringsgruppen for Normen (dato)
1.0	Første utgave av veilederen Personvern og informasjonssikkerhet i kontakten med pasient/bruker – En veileder av bruk av portalløsninger, SMS og e-post.	14. mars 2013
1.9	Oppdatering etter presisering om SMS i Normen 4.0 kap. 5.7.5: - Tatt inn innhold fra utgått faktaark 33 (e-post) - Oppdaterte definisjoner (lovhenvisninger) - Endret rekkefølge på kapitler. Teksten av kapittelet om SMS og e-post er likt strukturert. (Tatt inn opplisting over hva som kan sendes på e-post med presisering av at supplerende rutiner kan være nødvendig)	
2.0	- Formuleringen i kapittel 2.2 endret til "skal ikke avdelingsnavn som "…psykiatrisk politikk…", "benyttes"". - "Stilltiende" er tatt ut, og tilhørende omtale i 1.4 er endret. - Presisering om at vanlig e-post ikke skal benyttes til identifiserbare helseopplysninger er tatt inn først i kapittel 3. - En del mindre innspill fra Helse Nord er tatt inn i teksten.	12. februar 2015
3.0	Tredje utgave av veilederen med følgende endringer: - Forenkling av språk og struktur - Gjennomgående økt fokus på risiko og prosesser - Tabellene med Normens krav er tatt ut - Veilederen er gjort mer teknologinøytral - Lagt til et eget kapittel om implementering av nye løsninger - Sosiale medier er tatt inn i veilederen	02. februar 2020

Innhold

1 Innledning

1.1 Bakgrunn

Den teknologiske utviklingen har gitt helse- og omsorgstjenesten flere verktøy for å kunne kommunisere med pasienter og brukere. Mye informasjon går fremdeles via telefon og brev, men stadig større mengder med informasjon kan sendes via digitale verktøy. Pasienter har også endrede forventninger til interaksjon og tilgjengelighet på informasjon om sin helsetilstand.

Digital pasientkommunikasjon legger til rette for større grad av pasientmedvirkning, og kan effektivisere toveis og enveis kommunikasjon mellom helsepersonell og pasient/bruker. På denne måten kan både pasient og helsepersonell raskere få informasjon de har behov for, og forenkle kontakten med helsetjenesten.

Samtidig som digitale kommunikasjonsformer kan bidra til at pasienten mottar informasjon raskere, medfører bruk av kommunikasjonsteknologi at det oppstår nye risikoer for personvern og informasjonssikkerheten som virksomhetene må vurdere.

Digital pasientkommunikasjon kan understøtte pasientens eller brukerens rett til informasjon, jf. pasient- og brukerrettighetsloven § 2-3. Pasienten/brukeren har rett på informasjon som er nødvendig for å få innsikt i sin helsetilstand og innholdet i helsehjelpen, det vil si den behandling, pleie, omsorg, diagnostikk eller undersøkelse som tilbys eller ytes. En del av denne informasjonen kan gis gjennom digitale kommunikasjonsformer, forutsatt at taushetsplikten for helsepersonell ikke brytes.

Det finnes mange ulike måter å kommunisere digitalt med pasienter på, for eksempel SMS, e-post, brev til digital postkasse og meldinger via tjenesteportaler som helsenorge.no og private aktører.

Helsenorge er den offentlige kanalen for en samlet og sømløs tilgang til digitale tjenester innen den offentlige helse- og omsorgsektoren. Helsenorge brukes av en rekke virksomheter for å tilby innbygger administrative tjenester (for eksempel timebestilling), dialogtjenester (feks e-konsultasjon med fastlege) og innsynstjenester, som gir innbygger mulighet til å få innsyn i opplysninger om seg i registre og i pasientjournal.

Det finnes også en rekke andre portaler og innloggingsløsninger som pasienter kan benytte seg av for å sende eller motta informasjon fra helse- og omsorgstjenesten.

I tillegg til de overnevnte kommunikasjonsløsningene, ser man også en utvikling der virksomheter i helse- og omsorgssektoren tar i bruk sosiale medier i større grad enn tidligere. Denne veilederen vil derfor også ta for seg risiko ved bruk av sosiale medier.

De etiske perspektivene og hvorvidt det er fornuftig for en virksomhetet å ta i bruk sosiale medier vil ikke bli behandlet her. Det er allikevel utvilsomt at bruk av sosiale medier reiser noen nye problemstillinger som må vurderes. Veilederen vil derfor informere om sentrale problemstillinger, samt gi noen konkrete råd om hva virksomhetene bør vurdere.

1.2 Om veilederen

Tema for denne veilederen er informasjonssikkerhet og personvern ved bruk av digitale midler for kommunikasjon mellom helsetjenesten og pasienter og brukere. Veilederen tar også for seg risiko og risikoscenarier for de ulike kommunikasjonsteknologiene, samt ulike temaer innen personvern og informasjonssikkerhet, juridiske spørsmål og tiltak.

Formålet med veilederens innhold er å belyse grunnleggende spørsmål og prosesser virksomheten må ta stilling til for å oppnå god sikkerhet og ivaretakelse av personvernet, både i løsningen som benyttes og i kommunikasjonen i seg selv.

Veilederen retter seg i hovedsak mot mindre helsevirksomheter, men vil også være relevant for de større aktørene i sektoren.

Kapittel 2 omtaler grunnleggende krav og prosesser som må gjennomføres i arbeidet med digital pasientkommunikasjon. Kapittel 3 tar for seg implementering av nye digitale kommunikasjonsløsninger og krav til slike prosesser. Kapittel 4 omhandler risikovurdering og inneholder en ikke-uttømmende oversikt over scenarier som kan brukes i risikovurdering. Her vil man i tillegg finne nyttig informasjon til leverandører som utvikler slike kommunikasjonsløsninger.

Veilederens vedlegg inneholder eksempler på innhold i SMS og e-post.

I veilederen benyttes det enkelte uttrykk og definisjoner som er spesifikke for fagdisiplinene informasjonssikkerhet og personvern. Se Normens definisjonskapittel for forklaring.

1.3 Veilederens forhold til andre dokumenter og veiledere

Temaer som taushetsplikt, dokumentasjonsplikt og pasient- og brukerrettigheter omtales, men dekkes ikke uttømmende av denne veilederen. For veiledning om slike temaer vises det til følgende veiledninger og rundskriv:

- Helsepersonelloven med kommentarer
- Pasient- og brukerrettighetsloven med kommentarer
- Helsepersonells og forvaltningens taushetsplikt

Der denne veilederen overlapper eller har tilstøtende innhold med andre dokumenter i Normen:

- Veileder om bruk av video, lyd og bilde
- Veileder om de registrertes rettigheter
- Faktaark om behandlingsgrunnlag
- Veileder for små virksomheter
- Faktaark 24 – kommunikasjon over åpne nett
- Vedlegget til Normens krav som utgangspunkt for å utarbeide krav til leverandør
- Veileder om bruk av skytjenester

Veilederen går ikke inn på bruk av videokonsultasjon eller videokommunikasjon, men vil være relevant for systemer for videokonsultasjon der tjenesten har mulighet for chat eller annen skriftlig kommunikasjon mellom pasient og helsepersonell. For temaer innen video kan disse veilederne benyttes:

- Veileder i video-, lyd og bildeopptak: https://ehelse.no/normen/veiledere/veileder-video-lyd-og-bildeopptak-i-helse-og-omsorgssektoren
- Faktaark 54 – videokonsultasjon: https://ehelse.no/normen/faktaark/faktaark-54-videokonsultasjon
- Kvikk-guide for videokommunikasjon: https://www.ks.no/fagomrader/helse-og-omsorg/velferdsteknologi3/kvikk-guide-for-videokommunikasjon/

De kommunikasjonsformer som denne veileder tar for seg, forutsetter videre risikovurdering og selvstendig godkjenning i de enkelte virksomheter. Dette gjelder også for sosiale medier.

Veilederen tar ikke for seg informasjonsutveksling eller kommunikasjon om pasienter mellom virksomheter i helse- og omsorgssektoren.

Veilederen er ikke knyttet opp mot spesifikke leverandører, men det vil være beskrevet risikoscenarier som er spesifikke for en type kommunikasjonsteknologi.

1.4 Om Normen

Denne veilederen er et støttedokument under Normen som forvaltes av Styringsgruppen for Normen. Veilederen følger Normens forvaltningsmodell.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. I tillegg skal Normen bidra til å etablere mekanismer og regler som sikrer at virksomhetene kan ha gjensidig tillit til at øvrige virksomheters behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Her finner du en komplett oversikt over Normens krav og andre nyttige dokumenter.

En til enhver tid oppdatert versjon av veilederen finnes på www.normen.no. Dersom du har spørsmål knytte til veilederen kan du sende spørsmål og kommentarer til: normen@helsedir.no.

2 Overordnede prosesser

Dette kapittelet gir en innføring i grunnleggende prosesser og vurderinger som må gjøres før og under gjennomføring av kommunikasjon med pasienter og brukere. Denne delen er felles for alle områdene som dekkes av veilederen, og må leses i sammenheng med de spesielle risikoene som gjelder for hver kommunikasjonsteknologi, se kap. 4.

2.1 Kartlegging av faktiske forhold

For å kunne ta stilling til hvilke regler og retningslinjer som kommer til anvendelse for digital kommunikasjon med pasient/bruker, må virksomheten vurdere og kartlegge hva som faktisk gjøres i kommunikasjonen. Det innebærer at virksomheten må vurdere hva formålet med kommunikasjonen er, hva slags informasjon man sender og mottar, og hvordan informasjonen behandles i andre systemer.

Eksempler på spørsmål virksomheten kan stille seg er:

- Er det ytelse av helsehjelp?
- Er det ytelse av omsorgstjenester?
- Er det administrasjon av helsehjelp?
- Hvilken plikt har virksomheten til å dokumentere og/eller journalføre?
- Hvordan ivaretas dataminimeringsprinsippet?
- Er det risiko for formålsutglidning, slik at informasjon brukes til andre formål enn det som er tiltenkt?

Eksempel - faktiske forhold
En helsesykepleier på en helsestasjon ønsker å bruke sosiale medier for å kommunisere med ungdom. Formålet er å gi informasjon om kommunens helsetilbud, og tipse om andre tjenester som kan være nyttige å vite om. Helsesykepleieren er tilstede på det sosiale mediet i kraft av sin stilling som helsepersonell, og ikke som privatperson. Etter hvert som tjenesten blir kjent, begynner det å komme inn spørsmål om hjelp til helsesykepleierkontoen. Helsesykepleieren gir individuelle råd til brukerne, og mottar i den forbindelse store mengder helseopplysninger og annen sensitiv informasjon om brukerne hun kommuniserer med. Hun trekker ikke ut noe informasjon fra kontoen og loggfører heller ikke noe om kontakt eller hvilken oppfølging/råd som blir gitt.

- Er formålet en informasjonssamfunnstjeneste til ungdom eller individuell helsehjelp?
- Yter hun helsehjelp til de hun kommuniserer med?
- Har helsesykepleieren plikt til å dokumentere og journalføre sin kommunikasjon?
- Har hun dataansvar for helseopplysningene som hun får tilgang til?

Svarene på disse spørsmålene vil fortelle virksomheten mye om hva de faktisk gjør og hvilke krav og lovhjemler som kommer til anvendelse på den konkrete kommunikasjonen. Dersom virksomheten konkluderer med at de ikke bare administrerer helsehjelp, men også yter den, vil krav om journalføring og dokumentasjonsplikt være gjeldende. Hvis det behandles helse- og personopplysninger i kommunikasjonen må man også følge reglene i personopplysningsloven og personvernforordningen.

Selv om formålet med kommunikasjonsverktøyet er å gi informasjon, kan verktøyet i seg selv bidra til at den faktiske aktiviteten blir annerledes enn det som var den opprinnelige hensikten. Formålet med for eksempel sosiale medier er å være interaktive og har dermed funksjoner som aktivt oppfordrer til mer aktivitet fra brukerne. Virksomheten bør derfor sette seg godt inn i mediets natur og brukerkultur for å kunne være i stand til å forutse hva slags kommunikasjon man i realiteten legger til rette for. Dersom helsepersonell skal administrere løsningen, må virksomheten ha rutiner for hva man skal gjære hvis det er nødvendig å yte helsehjelp.

Eksempel – lukket gruppe på Facebook

Normbakken Rusklinikk ønsker å opprette en Facebook-gruppe for å holde kontakten med en gruppe av sine ruspasienter. Hensikten med gruppen er å invitere til sosiale aktiviteter, samt å gi pasientene venner og nettverk. Gruppen er lukket slik at ingen kan se hvem som er medlemmer, og gruppen er gitt et navn som ikke avslører at det er snakk om ruspasienter.

Etter hvert som tiden går, blir det åpenbart for klinikken at gruppen brukes som en plattform for kjøp og salg av narkotiske stoffer mellom brukerne. Det er også et tilfelle der en pasient skriver i gruppen og varsler om at han har tatt overdose. Klinikken reagerer i tide og skaffer livreddende helsehjelp til vedkommende.

I etterkant av dette bestemmer klinikken seg for å avvikle gruppen og finne en annen måte å kunne invitere til aktiviteter på.

2.2 Innledende vurderinger og risikovurderinger

2.2.1 Risikovurdering

Løsninger som brukes i forbindelse med digital pasientkommunikasjon skal risikovurderes opp mot nivå for akseptabel risiko. Det er risikovurderingen som ligger til grunn for alle de videre vurderingene og beslutningene; blant annet om man vil ta i bruk en kommunikasjonsløsning, hvilke typer behandling av personopplysninger som kan gjennomføres, hvilke tiltak som skal iverksettes, teknisk oppsett av teknologien, hvordan teknologien ivaretar personvernet og informasjonssikkerheten osv.

Risikovurdering skal gjennomføres før løsninger tas i bruk, ved større endringer eller om det oppstår vesentlige avvik. Om risikovurderingen viser uakseptabel risiko, skal løsningene ikke benyttes før risikoreduserende tiltak er iverksatt**.**

Alle løsninger for kommunikasjon med pasient eller bruker som behandler helse- og personopplysninger skal ha "egnede tekniske og organisatoriske sikkerhetstiltak" for å hindre brudd på informasjonssikkerheten. Brudd defineres som utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger.

Valg av egnede sikkerhetstiltak skal gjøres på bakgrunn av omfang og kategorier av opplysningene, pasientsikkerhet, aktuelt risikobilde mv. Tiltakene skal velges basert på risikovurderinger, og være forholdsmessige ut fra identifisert risiko.

I arbeidet med risikovurdering er det viktig å ha med ulike typer kompetanse: helsepersonell, juridisk, personvern, informasjonssikkerhet, drift, anskaffelse mm.

Eksempel på metode for risikovurdering, se Veileder om risikostyring i informasjonssikkerhet og personvern. Se kapittel 4 i denne veilederen for eksempler på risikoscenarier som kan benyttes i virksomhetens egen risikovurdering.

2.2.2 Personvernkonsekvensvurdering av løsninger for digital pasientkommunikasjon

Virksomheten skal alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte. Virksomheten skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet til den registrerte er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Hvis det da er sannsynlig at en behandling medfører høy risiko for de registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering, også kalt DPIA.

Digital kommunikasjon i helse og omsorg er en aktivitet som kan medføre høy risiko for de registrertes rettigheter og friheter. Særlig vil følgende aktiviteter i behandling føre til at virksomheten må gjennomføre DPIA:

- Når helseopplysninger behandles i stor skala
- Innføring av ny teknologi som ikke før er tatt i bruk av virksomheten
- Barn og andre sårbare grupper

Ikke alle kommunikasjonsløsninger vil medføre høy risiko for den registrertes rettigheter og friheter. I vurderingen av dette så kan det være aktuelt å vurdere:

- Omfang av personopplysninger
- Personopplysningenes art (hvem opplysningene gjelder, sensitivitet osv.)
- Kategorier av mottakere (deling, utlevering, innsyn osv.)
- Kategorier av behandlinger (innsamling, sammenstilling, lagring osv.)

Vurderinger av personvernkonsekvenser vil bero på en helhetsvurdering hvor en må ta stilling til kategorier av personopplysninger, behandlinger, mottakere, formålet og sammenhengen opplysningene behandles i. Om virksomheten gjør denne helhetsvurderingen basert på punktene over kan virksomhetene komme frem til gode avgjørelser. Resultatet av en DPIA vil også bero på en avveining av behandlingen sett opp mot risikominimerende tiltak som vil gjøre behandlingen mer inngripende. Eksempler på slike tiltak kan være at opplysninger ikke blir lagret og at man har rutinger for sletting av overskuddsinformasjon.

Tilsvarende som ved gjennomføring av risikovurdering er det viktig å ha med bredt sammensatt kompetanse når vurderingen skal gjøres. Ved gjennomføring av DPIA vil det også være aktuelt å involvere representanter for de registrerte, for eksempel en pasient eller et pasientombud.

Dersom virksomheten kommer frem til at det ikke er behov for å gjennomføre en full DPIA, må dette dokumenteres og være saklig begrunnet.

Det finnes mange gode maler for DPIA, f.eks. mal fra Direktoratet for e-helse og mal fra KINS/Bærum kommune. Se kapittel 4 for eksempler på scenarier som kan brukes i en personvernkonsekvensvurdering.

Eksempel – bruk av sosiale medier og DPIA

Normgata Helsestasjon ønsker å få større kontakt med ungdommene i kommunen og er på utkikk etter en løsning som gjør at de kan være til stede på en plattform som ungdom i

aldersgruppen 13-19 bruker. Formålet med å bruke sosiale medier er å gi informasjon og engasjere målgruppen.

Helsestasjonen gjennomfører en kartlegging av sosiale medier og kommer frem til at Instagram er best egnet for formålet og er godt utbredt i målgruppen.

Normgata helsestasjon gjennomfører flere vurderinger (bl. a. risikovurdering av applikasjonen og helsefaglige vurderinger) for å sikre at løsningen ivaretar krav til informasjonssikkerhet og personvern. De vurderer konsekvensene for personvernet til ungdommene, og om de har behandlingsgrunnlag. De gjør videre en initialvurdering for å finne ut om behandlingen innebærer høy risiko for de registrerte, for å finne ut om de burde gjøre en fullskala personkonsekvensvurdering.

Nedenfor følger noen momenter som Normgata helsestasjon inkluderer i vurderingen:

- Det er viktig å skaffe seg kunnskap om hvordan det konkrete mediet brukes, og hva slags kultur som eksisterer blant brukerne. På Instagram er det for eksempel vanlig å tagge andre brukere i kommentarfelt, for å gjøre dem oppmerksom på innholdet i posten. Dette er en mulighet som kan misbrukes. Dersom kontoen til helsestasjonen publiserer et innlegg om kjønnssykdommer eller angstlidelser, er det en risiko for at en bruker tagger en annen bruker i kommentarfeltet med kommentarer som "Dette bør du sjekke ut" eller lignende. Slike hendelser kan være uskyldig moro, men kan også opplevelses svært krenkende og inngripende for den det gjelder, og potensielt få konsekvenser for omdømmet til den som blir rammet.
- En annen risiko med sosiale medier som har åpent kommentarfelt, er at man ikke har noen kontroll over hva som kan publiseres der. En følger kan for eksempel kommentere at de har angst eller andre plager, og dermed avsløre sensitiv informasjon om seg selv. Det er også en risiko for at det kan avdekkes sensitiv informasjon om andre identifiserbare personer.
- Selv om helsestasjonen selv sletter kommentarer og direktemeldinger, har de ikke selv kontrollen over hvor lenge de "brukerslettede" meldingene bevares av løsningen/leverandøren.
- Instagramkontoen retter seg mot ungdom som er i en sårbar periode av livet og som skal nyte et sterkt vern.
- Applikasjonen har mulighet for direkte meldinger, der brukere kan kontakte helsestasjonskontoen og gi sensitiv informasjon og helseopplysninger om seg selv og andre. Det burde undersøkes om muligheten for direktemeldinger skal begrenses eller stenges.
- Kontoen kan få flere følgere enn tiltenkt dersom kontoen blir populær og risikoen for at det publiseres sensitivt innhold vil dermed øke.
- Det følger av brukervilkårene at Instagram blant annet kan lagre kopier av alle bilder som publiseres og bruke de til egne formål, for eksempel reklame
- Eventuell aktivitetsdata fra brukerne som liker eller kommenterer innhold vil kunne brukes av Instagram til å tilby mer spisset innhold til brukeren.
- Bruk av sosiale medier kan medføre overføing av personopplysninger til tredjeland.

Basert på en initialvurdering av personvernkonsekvenser bestemmer helsestasjonen at det skal gjennomføres en fullskala DPIA for denne aktiviteten, da de blant annet konkluderer med at behandlingen medfører høy risiko for de registrerte, den omfatter en sårbar gruppe personer, og at det finnes få tiltak som kan redusere risikoen betraktelig.

2.2.3 Særlig om vurderinger av sosiale medier

Det vil være vanskelig for virksomheter å oppfylle enkelte av Normens krav ved bruk av sosiale medier. Dette på grunn av blant annet krav til autentisering og autorisering i hovedsak er rettet mot behandlingsrettede helseregistre. Derfor vil det være desto viktigere at virksomheten gjør en grundig risikovurdering (eventuelt også personvernkonsekvensvurdering, se. Kap 2.2.2) og implementerer risikoreduserende tiltak.

Forslag til vurderingstemaer og risikoscenarier som kan brukes i risikovurdering finnes i dette kapittelet, i tillegg kan det være aktuelt å vurdere risikoscenariene som er beskrevet i kapittel 5.

Det er viktig at vurderingene virksomheten gjør løftes i organisasjonen, slik at virksomhetens ledelse har eierskap til beslutningen og har forståelse for risikoen som det sosiale mediet innebærer for virksomheten.

Dersom virksomheten ønsker å ta i bruk sosiale medier er det en rekke problemstillinger som det bør tas stilling til, for eksempel:

- Alle sosiale medier har sin egen internkultur for bruk, som varierer med aldersgruppe. Unge mennesker bruker sosiale medier på en annen måte enn eldre mennesker og til andre formål.
- De fleste sosiale medier har flere kanaler som kan brukes. Selv om virksomheten selv tenker å kun publisere informasjon til publikum, kan funksjoner som kommentarfelt, tagging og direktemeldinger brukes til å publisere personlig og sensitiv informasjon.
- Mange sosiale medier har svært omfattende brukervilkår som kan være vanskelig å få oversikt, slik at data kan brukes til formål som virksomheten ikke kan kontrollere eller forutsette. Disse vilkårene kan også oppdateres uten varsel.
- Ved bruk av sosiale medier kan offentlige aktører understøtte innsamling av brukerdata og markedsføring fra private kommersielle aktører
- Hvilket ansvar har virksomheten for innholdet som blir publisert? Hvilket ansvar har virksomheten for å sørge for moderering og sletting av innhold?
- Ivaretakelse av taushetsplikten på sosiale medier.
- Hvordan skal virksomheten ivareta de registrertes rettigheter?

Eksempel på problemstilling ved risikovurdering av sosiale medier

Barselavdelingen på Normland sykehus ønsker å opprette en Instagram-konto for avdelingen. Hensikten er å vise frem for publikum hvordan de jobber, og vise små glimt fra hverdagen til de ansatte.

Det er på forhånd bestemt at ingen pasienter, pårørende eller andre besøkende skal være synlige på bilder eller videoer som postes fra avdelingen, og ansatte må samtykke til publisering av bilder/video.

Under et møte hvor det gjennomføres risikovurdering av applikasjonen, kommer en ansatt på et nytt scenario: Hva hvis innholdet som publiseres er med på generere målrettet reklame for brukere som følger kontoen? Hun viser til at hun har fått målrettet reklame for blant annet leker og annet utstyr til barn etter å ha fulgt lignende kontoer tidligere. Hun har også fått målrettede annonser rettet mot barn og foreldre for mer alternative produkter som ikke har noen dokumentert medisinsk effekt, blant annet healingkrystaller for babyer. Hun

har også fått opp nyhetsartikler som sier at morsmelkerstatning er skadelig og at babyer skal sove på magen.

Hvordan skal sykehuset ta stilling til denne risikoen?

2.2.4 Hensynet til pasienter og brukere ved valg av kommunikasjonsform

For å kunne ivareta kravet til forsvarlig helsehjelp, må virksomheten vurdere om digital pasientkommunikasjon kan komme i konflikt med dette kravet. Ved implementering eller bruk av digitale løsninger for kontakt med pasienter og brukere, bør virksomheten gjøre en vurdering av om den aktuelle teknologien er hensiktsmessig for å kommunisere med sin pasientgruppe. Ulike pasienter og pasientgrupper har ulike behov og utfordringer som må adresseres og hensyntas når man velger kommunikasjonsmetode.

Eldre pasientgrupper vil eksempel kunne ha større utfordringer med å ta i bruk ny teknologi eller autentiseringsmetoder. Ruspasienter kan være utfordrende å få tak i, og enkelte pasienter eller brukere har ikke bank-ID eller annen elektronisk ID som trengs for å tilegne seg informasjonen virksomheten prøver å gi.

Virksomheten bør ha en rutine for å formidle informasjon om timeavtaler, prøvesvar eller annen type informasjon som det er viktig at pasienten eller brukeren får kunnskap om, dersom pasienten ikke kan eller klarer å bruke de digitale verktøyene som virksomheten benytter seg av.

Virksomheten må videre sørge for at det er etablert rutiner som ivaretar at meldingen/informasjonen til pasienten ikke er inngripende og krenker personvernet, men samtidig har tilstrekkelig informasjon til pasienten. Innholdet i kommunikasjonen må utformes på en slik måte at innholdet er tydelig for pasienten. Det må for eksempel komme tydelig frem hva som menes eller hva pasienten må foreta seg for å tilegne seg informasjonen.

Virksomheten må alltid foreta en vurdering om innholdet i kommunikasjonen kan avsløre mer informasjon enn det som er tiltenkt og bryte med reglene om taushetsplikt. En melding fra fastlegen om ny time vil ikke kunne regnes som sensitiv informasjon hvis meldingen ses av andre, men en melding om time hos en spesifikk avdeling på et sykehus kan avsløre informasjon om pasientens helsetilstand.

Samtidig må man ta hensyn til andre forhold, for eksempel at et sykehus kan være stort og bestå av flere bygninger. Det vil da kunne være hensiktsmessig å gi informasjon om hvor pasienten skal henvende seg når han eller hun møter opp til timen sin.

Videre må virksomheten vurdere muligheten for andre typer hendelser, for eksempel verktøy som øker risikoen for menneskelige feil, både hos helsepersonellet og pasienten.

Eksempel – feilsending av e-post
Et stort forskningsprosjekt følger pasienter som har blitt utsatt for overgrep som barn. Alle pasientene er nå voksne, og formålet med studien er å undersøke i hvilken grad pasientene påvirkes av disse hendelsene senere i livet. Ingen av pasientene vet hvilke andre som deltar i studien.

Forskerne skal sende ut et nytt skjema som pasientene skal fylle ut, som et ledd i studien. Skjemaet skal sendes ut på e-post til pasientene. En menneskelig feil medfører at samtlige e-postadresser settes inn i til-feltet, og ikke i blindkopi-feltet. Dette medfører at identiteten til mange av pasientene i studien avsløres, da de fleste bruker fullt navn som e-postadresse.

Situasjonen forverres ytterligere ved at mange av pasientene som sier i fra om hendelsen benytter seg av "svar-alle"-funksjonen, slik at e-postadressene til pasientene fortsetter å sirkulere.

I dette tilfellet er det nærliggende å fastslå at forskerne bak studien burde ha valgt en annen måte å kommunisere med pasientene, der risikoen for feilsending var lavere enn med e-post. Eksemplet illustrerer også at i en risikovurdering må man vurdere risikoen for brukerfeil, slik at virksomheten eller pasienten ikke uaktsomt deler sensitiv informasjon med andre. Ved feilsending eller annen deling av sensitiv informasjon må også hendelsen meldes som avvik til Datatilsynet.

2.3 Lovlig behandling av personopplysninger

2.3.1 Behandlingsgrunnlag

Personvernforordningen stiller krav om at all behandling av personopplysninger skal ha et lovlig grunnlag. Dette kalles behandlingsgrunnlag. Det lovlige grunnlaget kan finnes i andre lover enn personvernforordningen. Behandlingsgrunnlaget skal dekke alle typer behandlinger av helse- og personopplysninger som utføres: innsamling, registrering, lagring, sletting, utlevering, mv.

Utgangspunktet for å kunne dokumentere helse- og personopplysninger i helse- og omsorgstjenesten, er at opplysningene er relevante og nødvendige for å kunne yte eller administrere helse- og omsorgstjenester. Dokumentasjon av opplysninger for andre formål, eller innenfor andre sektorer (f.eks. på skolen eller i barnevernet) må ha et annet behandlingsgrunnlag, enten i sektorlovgivningen eller direkte i personvernforordningen.

For mer veiledning om behandlingsgrunnlag, se Normens kapittel 4.1. Veileder for rettigheter ved behandling av helse- og personopplysninger. For mer om samtykke til helsehjelp se pasient- og brukerrettighetsloven med kommentarers kapittel 4,

2.3.1.1 Samtykke til bruk av portaler og applikasjoner

Enkelte helsevirksomheter har innloggingsportaler på sine nettsider hvor pasienten kan logge inn med sikker autentiseringsløsning (i praksis med Bank-ID eller MinID) for å få tilgang til timebestilling, reseptfornying, digital meldingsboks mm. Enkelte portaler kan også benyttes via applikasjon til smarttelefon.

Bruken av slike nettportaler/applikasjoner krever samtykke fra pasienten. Det er kun nødvendig å innhente samtykke til behandling av personopplysninger som er nødvendige for å bruke selve portalen eller plattformen. Eksempler på slike opplysninger kan være

fødselsnummer, samtykker gitt av pasienten eller andre innstillinger som styrer bruk av plattformen, samt opplysninger som pasienten selv velger å registrere, slik som SMS-varsel mm. Samtykket bør skilles ut til de enkelte tjenestene som finnes i portalen/applikasjonen, slik at pasienten kan samtykke til å motta for eksempel påminnelser på e-post, men ikke på SMS.

Det er ikke nødvendig å innhente samtykke til behandlingen av helseopplysninger som gjøres tilgjengelig for pasienten via portalen, da dette er en rettslig plikt for helsetjenesten som faller inn under dokumentasjonsplikten.

Administrasjon av samtykket for bruk av plattformen eller portalen bør kunne gjøres i nettportalen/applikasjonen. Hvis ikke må pasienten informeres om hvor vedkommende skal henvende seg for å trekke sitt samtykke, for eksempel ved å kontakte helsevirksomheten. Dette bør det gis informasjon om til pasienten ved første gangs pålogging til tjenesten.

For mer informasjonen om kravene til samtykke og administrering av samtykke, se Veileder for rettigheter ved behandling av helse- og personopplysninger.

2.3.2 Taushetsplikt

Personell som behandler helse- og personopplysninger i helse- og omsorgstjenesten, vil være underlagt regler om taushetsplikt. Dette bidrar til at den registrerte kan være trygg på at informasjonen ikke blir gitt videre til uvedkommende. Taushetsplikten gjelder også for personopplysninger som fremkommer i digital pasientkommunikasjon.

Virksomheten skal legge til rette for at alle medarbeidere til enhver tid er bevisst taushetspliktens innhold og omfang. Virksomheten skal sørge for praktiske løsninger, inkludert teknologiske, som gjør at taushetsplikten kan etterleves av medarbeiderne. Dette innebærer for eksempel rutiner for å sikre at informasjon kommer frem til rett mottaker, og at virksomheten etablerer tiltak for å forhindre at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten tilgjengeliggjøres ved hjelp av ukryptert e-post og SMS eller andre usikre kanaler.

Les mer om taushetsplikten generelt på temasidene for taushetsplikt og opplysningsplikt på Helsedirektoratets nettsider.

2.4 Tilgangsstyring[1], autorisering og autentisering

2.4.1 Tilgangsstyring

Virksomheten skal ha rutiner for autorisering, endring og avslutning av tilganger til verktøy som benyttes til pasientkommunikasjon. Tilgangsstyring skal etableres for alle informasjonssystemer. Det gjelder også for administrator- og systembrukere. Bare autorisert personell med tjenstlige behov skal få tilgang til helse- og personopplysninger.

Innenfor rammen av taushetsplikten skal virksomheten sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og samarbeidende personell når dette er nødvendig for å yte eller administrere helsehjelp til den enkelte.

Virksomheten bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten og personvernet.

[1] Faktaark 14 - tilgangsstyring

2.4.2 Autorisering

Virksomheten er ansvarlig for at autorisasjoner tildeles, administreres og kontrolleres. Ved tildeling av autorisasjon skal lovbestemt taushetsplikt vurderes og ivaretas.

Det er kun autorisert personell som skal ha tilgang til å benytte seg av digitale verktøy for pasientkommunikasjon. I helsevirksomheter hvor man har ulike typer helsepersonell, for eksempel et helsesenter med leger og fysioterapeuter som benytter samme EPJ-system, må de ha ulike roller.

2.4.3 Autentisering[2]

Autorisert personell skal bekrefte sin identitet på en sikker måte, det samme gjelder for pasienter.

Sikkerhetsnivået for autentisering må fastsettes på grunnlag av en risikovurdering. I risikovurderingen må man blant annet ta hensyn til løsningen som benyttes og hva slags opplysninger som skal behandles.

Autentisering for bruk av kun administrative funksjoner uten helse- og personopplysninger (for eksempel bestilling og avbestilling av time uten at grunnen for timebestilling oppgis), skal gjøre med minimum **sikkerhetsnivå betydelig.[3]**

For autentisering for tilgang til og kommunikasjon av helseopplysninger i nasjonale løsninger (for eksempel Helsenorge) eller løsninger levert av helsepersonell (inklusive timebestilling der pasient/bruker oppgir grunnen for bestilling av ny time og reseptfornying) kreves **sikkerhetsnivå høy.[4]**

For løsninger til private formål (helsepersonell er ikke involvert) anbefales autentisering med **sikkerhetsnivå betydelig.**

2.5 Gi pasienten god informasjon om kommunikasjonen

Det må være forutsigbart for pasientene i hvilke kanaler de vil kommunisere med helsetjenesten. Uklarhet kan resultere i at helsetjenesten mottar sensitiv informasjon i usikre kanaler, som til postmottak eller helsepersonells private kontoer på sosiale medier. Mottak av sensitiv informasjon i usikre kanaler vil også medføre at virksomheten må bruke ressurser på å håndtere og slette informasjonen. Det må derfor informeres tydelig om hvilke kanaler pasienter og brukere kan benytte seg av for oversending av informasjon som har betydning for helsehjelpen som gis.

Det kan gis slik informasjon på ulike måter, for eksempel at det fremkommer på virksomhetens kontaktnettsider eller som default "melding" når pasienten åpner et chatvindu. Pasienten kan også informeres under opphold på sykehus eller ved besøk hos fastlegen.

I tillegg til informasjon om hvilke kanaler som blir benyttet, må pasienten/brukeren vite hvordan han eller hun skal autentifisere seg, for eksempel om løsningen/appen bruker bank-ID eller andre metoder for sikker autentisering.

---

[2] eIDAS-forordningen (910/2015) erstattet e-signaturdirektivet og ble inntatt i norsk rett 15.06.2018. ID-porten og bank-ID er anerkjent som e-ID-ordning under dette direktivet.
[3] Tilsvarer sikkerhetsnivå 3.
[4] Tilsvarer sikkerhetsnivå 4.

2.6 Rettigheter

Som pasient og bruker har man en rekke rettigheter som i hovedsak kan deles i to: pasientrettigheter og personvernrettigheter.

Pasientrettighetene finnes i pasient- og brukerrettighetsloven, og inneholder rettigheter som innsyn i journal, retten til forsvarlig helsehjelp og retten til fritt behandlingsvalg.

Personvernrettighetene har som mål å gi den enkelte kontroll over sine helse- og personopplysninger, og finnes i personopplysningsloven og personvernforordningens kapittel 3.

I arbeidet med digital pasientkommunikasjon er virksomhetens ansvarlig for at den det kommuniseres med får oppfylt sine rettigheter. I Normen kap. 4 er disse formulert som plikter for virksomheten.

Informasjon om de registrertes personvernrettigheter utover det som dekker pasientkommunikasjon spesielt, finner du i Veileder for rettigheter ved behandling av helse- og personopplysninger. Informasjon om pasientrettigheter generelt finner du i pasient- og brukerrettighetsloven med kommentarer på Helsedirektoratets nettsider.

2.7 Styringssystem og rutiner

Alle virksomheter skal ha et styringssystem for informasjonssikkerhet og personvern. Styringssystemet skal omfatte virksomhetens arbeid med digital pasientkommunikasjon.

Virksomheter i helse- og omsorgssektoren som skal ha løsninger for digital pasientkommunikasjon må etablere rutiner for bruk og drift av løsningene. Tabellen nedenfor er et forslag til hvilket innhold overordnede rutiner virksomheter i sektoren bør ha. Dette kan være et utgangspunkt for tilpassede rutiner for egen virksomhet og valgt løsning.

Nr	Rutine	Forslag til innhold
1.	Tilgangsstyring	• Endre tilganger • Avslutning av tilganger
2.	Autorisering og autentisering av pasient	• Beskrivelse av hvordan pasient autoriseres • Beskrivelse av hvordan pasient autentiseres for å sikre entydig identifisering
3.	Autorisering og autentisering av helsepersonell.	• Autorisere helsepersonell til tjenstlig behov • Beskrivelse av hvordan helsepersonell autoriseres • Beskrivelse av hvordan helsepersonell autentiseres på en sikker måte
4.	Kryptering av kommunikasjon	• Jevnlig kontroll av at kommunikasjon er kryptert • Dersom dekryptering er nødvendig, må virksomheten ha rutiner for hvordan dette skal gjennomføres. Se Normen kapittel 5.3.5
5.	Rutiner for å sikre at meldinger sendes til rett mottaker.	• Virksomheten bør benytte til kontakt- og reservasjonsregistret hvis den har tilgang til dette.
6.	Periodisk kontroll av tildelte rettigheter	• Kontroll av tildelte rettigheter for helsepersonell • Kontroll av tildelte rettigheter for administratorbruker
7.	Journalføring av helse- og personopplysninger	• Ansvar for journalføring • Hva som skal journalføres • Tidspunkt for journalføring

Nr	Rutine	Forslag til innhold
8.	Bruk av helsepersonellets private utstyr ved pasientkommunikasjon (mobiltelefon, nettbrett, PC)	• Minimumskrav til utstyret • Sikring av helse- og personopplysninger på utstyret
9.	Informasjon og opplæring av helsepersonell	• Temaer i opplæringen; bruk av løsningen, hva som kan/ikke kan sendes via løsningen, taushetsplikt informasjonssikkerhet og personvern • Tidspunkt for opplæring • Rutiner som ivaretar at meldingen til pasienten ikke er inngripende og krenker personvernet, men samtidig har tilstrekkelig informasjon til • pasienten
10.	Informasjon til pasient	• Temaer i informasjon; bruk av løsningen, hvilke kanaler som brukes.
11.	Andre rutiner som må vurderes dersom løsningen krever det	Administratortilganger • Administratorbrukere som skal etableres • Systembrukere som skal etableres • Krav til personlig brukerkonto for administratortilgang • Autorisering av administratortilgang Autentisering av administratortilgang Autorisering og autentisering av helsepersonell • Ulike ansettelsesforhold skal identifiseres • Tidsbegrensning av autorisasjonen Registrering av tildelt autorisasjon i autorisasjonsregister
12.	Rettigheter	• Beskrivelse av hvordan pasient- og personvernrettigheter skal ivaretas.
13.	Tilgjengeliggjøring av informasjon til pasient	• Sørge for at helse- og personopplysninger stilles til rådighet på en slik måte at pasient/bruker ikke er avhengig av å laste ned/lagre opplysningene på eget utstyr for å gjøre seg kjent med informasjonen.
14.	Melding av avvik	• Hvem som melder avvik og hvordan dette skal melding og varsles i virksomheten.
15.	Sosiale medier	• Hvordan virksomheten sørger for lovlig grunnlag (behandlingsgrunnlag) for behandlingen av helse- og personopplysninger i sosiale medier • Hvordan og når en behandling skal føres i virksomhetens protokoll. • Hva slags informasjon som skal gis ved publisering av personopplysninger og innhenting av samtykke, inkludert publisering av bilder • Retningslinjer for hva som kan og ikke kan publiseres

Nr	Rutine	Forslag til innhold
		• Prosess for tilgangsstyring og hvordan passord skal oppbevares • Prosess for hvordan innhold på sosiale medier skal modereres, for eksempel hvis en følger av siden publiserer innhold med sensitiv informasjon eller bruker chat-funksjonen til å skrive inn sensitiv informasjon • Hva helsepersonell skal foreta seg dersom de blir kontaktet direkte av pasienter eller brukere • Hvordan de registrertes rettigheter skal ivaretas, for eksempel sletting. Se Normens veileder om de registrertes rettigheter.

2.7.1 Eksempler på rutiner i praksis

Eksempel på avvikshåndtering:
Pasient NN er 16 år og er pasient ved Normland sykehus. I forbindelse med en oppdatering av sykdomsbildet, skal sykehuset sende en oppdatering til de pårørende. Pasienten har samtykket til at denne informasjonen gis. Ved en feil sendes denne informasjonen til en rekke andre pårørende i tillegg til rett mottaker. Pårørende til NN får vite dette via andre som har mottatt informasjonen, da lokalsamfunnet er lite, og alle kjenner alle.

Pårørende til NN blir svært opprørte, og kontakter sykehuset for å få informasjon om det som har skjedd. Sykehuset har ikke oppdaget feilen tidligere, men tar affære og melder avviket til Datatilsynet. De vurderer avviket til å ikke være så alvorlig at det er nødvendig å varsle de registrerte.

De pårørende kontakter sykehusets personvernombud for å få bistand. De mener at de har rett på mer informasjon om det som har skjedd, og synes det er svært ubehagelig at andre i lokalsamfunnet har fått sensitiv informasjon om sønnen deres. De vil derfor, i tillegg til informasjon om avviket, ha kontaktinformasjon til de andre mottakerne.

Personvernombudet kontakter egen virksomhet og argumenterer for at de pårørende bør få varsel etter artikkel 34, da de allerede er kjent med at avviket har skjedd og hva slags informasjon som er på avveie. Videre er det et viktig poeng å demonstrere at man tar hendelsen på alvor og at man gjør det man kan for å ivareta pasienten og de pårørende. I en ubehagelig situasjon som denne er det avgjørende at pårørende og NN føler at de blir sett og at deres ubehag ikke bagatelliseres som en "menneskelig feil". Personvernombudet anbefaler at virksomheten tar hensyn til dette i sin kontakt med NN og de pårørende, og ikke bare vise til at "reglene er sånn". Ombudet mener allikevel at man ikke kan gi ut informasjon om andre mottakere, da disse har en selvstendig rett til å få sitt personvern ivaretatt.

Hendelsen resulterer i at sykehuset gjør endringer i sine informasjonsrutiner, og fra nå sender informasjon via andre kanaler der risikoen for feilsending vurderes å være mye lavere. Sykehuset følger opp NN og hans pårørende ved å kontakte dem direkte og informere om rutineendringen, for å gjøre dem trygge på at dette ikke vil skje igjen.

Eksempel :
En legesekretær ved Normland Legesenter skal sende ut SMS med informasjon om at prøvesvaret til en pasient er klart. Legesekretæren er nyansatt og dermed litt usikker på hvordan meldingen skal utformes slikt at hun ikke bryter taushetsplikten.

Etter å ha tenkt seg litt om slår hun opp i legesenterets rutiner for sending av informasjon, som heldigvis er oppdaterte. Det finnes en egen rutine for sending av 1:1-meldinger til pasienter, herunder SMS.

Rutinen sier blant annet at:

- Avsender på SMSen vil være "Normland Legesenter".
- Det er viktig at meldinger til pasient ikke utformes slik at den avslører informasjon om diagnoser eller annet om pasientens helsetilstand. Henvis heller pasienten til legesenterets sikre nettportal der pasienten kan logge inn med Bank-ID og se prøvesvaret sitt.
- SMS skal ikke brukes for å informere om resultatet av prøvesvar eller diagnoser, da det ikke er sikkert at mobiltelefonen kun brukes av pasienten.

Legesekretæren sender følgende SMS til pasienten: "Du har fått et nytt prøvesvar. Logg inn på Normland.no med Bank-ID for å se prøvesvaret ditt.
Vennlig hilsen Normland Legesenter".

2.7.2 Bruk av private og personlige enheter

Det forekommer tilfeller der helsepersonell benytter seg av sin private enhet, for eksempel mobiltelefon, i utførelsen av sitt arbeid. Et eksempel kan være en lege som mottar eller sender pasientinformasjon til annet helsepersonell, eller som kommuniserer direkte med pasienten sin over SMS eller e-post.

Det må skilles mellom enheter som er private, og personlige enheter som er utlevert av arbeidsgiver med den hensikt å brukes på jobb. Sistnevnte vil være underlagt arbeidsgivers styringsrett, og arbeidsgiver vil kunne bestemme formålet med bruken og hva enheten konkret skal brukes til. Den tilsiktende bruken må være risikovurdert, ligge i virksomhetens styringssystem og det må finnes rutiner for bruken. Dersom en personlig enhet for eksempel kun brukes til å ringe internt på avdelingen, men de ansatte også ønsker å sende SMS med røntgenbilder til kollegaer, må dette risikovurderes før sending av bilder kan starte.

Dersom virksomheten anskaffer egne mobiltelefoner til de ansatte der formålet er telefonisk pasientkontakt, vil det være en risiko for at man for eksempel mottar SMS med sensitiv informasjon. Her vil et aktuelt risikoreduserende tiltak være å anskaffe ikke-smarttelefoner, og ha rutiner for sletting av mottatte SMS etter mottak, eventuelt etter at dokumentasjonspliktig informasjonen er registrert i virksomhetenes systemer.

Ved bruk av personlig arbeidsenhet er det noen særskilte risikoer som må vurderes., blant annet:

- Hvordan man kan slette informasjonen i etterkant, både lokalt og i eventuell backup
- Hvordan man sikrer at andre ikke får tilgang til informasjonen – sikring av enheten
- Hvordan man forholder seg hvis enheten mistes eller kommer på avveie

- Hvordan man får journalført eventuell informasjon som fremkommer i kommunikasjonen

Bruk av private enheter har i tillegg til eksemplene over noen særskilte risikoer:

- Hvordan man skiller arbeidsrelatert informasjon fra privat informasjon
- Sletting av data fra enheten, inkludert tilhørende skylagring
- Formålsutglidning skjer ved at den ansatte tar i bruk enheten til oppgaver som ikke er risikovurdert
- Hvordan man beskytter informasjon som er lagret på enheten dersom uvedkommende får tilgang eller hvis enheten mistes eller blir stjålet

Eksempel:
En lege ved Normland legesenter mottar en SMS fra en pasient på sin private mobiltelefon. Pasienten har funnet nummeret til legen via en nummeropplysningstjeneste, og oppgir mye sensitiv informasjon til legen vedrørende sin helsetilstand. Pasienten hadde vært på konsultasjon tidligere på dagen og ønsket å legge til noen opplysninger han hadde glemt å opplyse om.

Hva skal legen gjøre med informasjonen og SMS-en?

Legen er litt usikker på hvordan han skal forholde seg til SMS-en og innholdet som står i den. Informasjonen pasienten opplyser om virker utvilsomt relevant for den videre behandlingen. Det er ingenting som tilsier at det er en akuttsituasjon. Heldigvis har Normland Legesenter gode internrutiner for hvordan slike tilfeller skal håndteresRutinen inkluderer blant annet å slette SMS og alle andre steder meldingen kan være lagret

Legen svarer pasienten at han må ringe legekontoret og bestille en ny legetime, slik at opplysningene kan følges opp på riktig måte. Deretter sletter han SMS-en lokalt på telefonen. I tillegg sørger legen for å slette backup av meldingen i skyen som er tilknyttet sin smarttelefon.

2.7.3 Nødrettsbetraktninger

Det kan tenkes tilfeller der en nødsituasjon kan gjøre det nødvendig å kontakte eller sende informasjon til en pasient eller bruker via et annet verktøy/system enn det som er angitt i virksomhetens rutine. Det kan også tenkes tilfeller der man har behov for å sende mer informasjon enn det som vanligvis er nødvendig.

Dette er uheldig, men kan ut fra en nødrettsbetraktning av og til være nødvendig for å gi pasienten trygg og rask behandling. At helsepersonellets privattelefon og utradisjonelle tiltak benyttes i kritiske situasjoner kan forsvares i enkelttilfeller, men når dette går over i en systematisk praksis berører det virksomhetens systemansvar etter spesialisthelsetjenesteloven § 2-2 og § 3-2.[5]

Man bør først og fremst benytte seg av telefonisk kontakt med pasient i et nødstilfelle, da kanaler som e-post, SMS og sosiale medier ikke har garantert leveranse.

[5] Rundskriv om informasjonshåndtering i spesialisthelsetjenesten.

Eksempelvis kan det være nødvendig å gi rask informasjon om endringer i legemiddelbruk eller få tak i en pasient svært raskt av ulike grunner. Det vil da kunne være riktig å avvike fra rutiner for å kunne gi forsvarlig helsehjelp. Hvis det derimot er vanlig å bruke andre verktøy/system enn det som er angitt i virksomhetens rutine for å kommunisere med pasient, bør det gjenspeiles i rutinene når dette kan gjøres og ikke. Det bør også gjøres en vurdering om det kan gjennomføres tiltak for å forhindre at slike kreative metoder for pasientkommunikasjon er nødvendige. Dette er både av hensyn til personvernet, informasjonssikkerheten og pasientsikkerheten.

3 Implementering av nye kommunikasjonsverktøy

3.1 Innledning

Dersom virksomheten skal gjøre innkjøp av nye løsninger for pasientkommunikasjon, er det en rekke prosesser og vurderinger som virksomheten må igjennom for å sørge for god og sikker implementering.

Kravstilling og nødvendige sikkerhetstiltak inngår i alle anskaffelser og implementeringsprosesser, og virksomheten må sørge for at den har tilstrekkelig kompetanse tilgjengelig.

For oversikt over grunnleggende prosesser som virksomheten må gjennomføre, se kapittel 2.

Eksempel på implementeringsprosess:

Normbakken legekontor fått en tilbud fra sin EPJ-leverandør om å kjøpe en kommunikasjonsmodul til sitt eksisterende system. Legekontoret ønsker å ta i bruk modulen for å lette arbeidet med administrasjon av blant annet timebestilling og reseptfornying. Flere pasienter har etterlyst en slik mulighet, fremfor å måtte ringe til legekontoret. Modulen har også muligheter for å sende enkle meldinger til en egen pasientpostkasse, og pasienten kan sende informasjon til legekontoret gjennom løsningen. Leverandøren tilbyr også en mobilapplikasjon som pasienten kan velge å benytte seg av.

Etter at det er besluttet å kjøpe inn modulen, gjør Normbakken legekontor innledende vurderinger av kommunikasjonsmodulen, som risikovurdering og helsefaglige vurderinger.

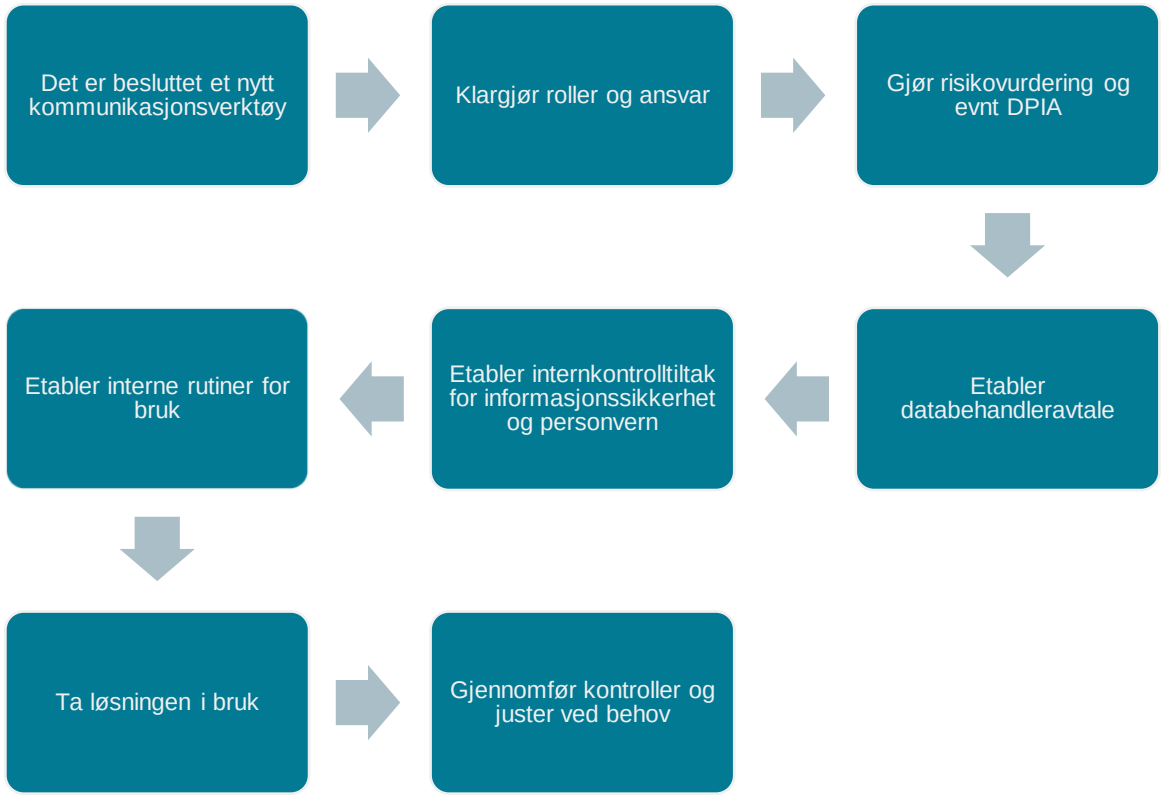
Etter en initialvurdering blir det besluttet å gjennomføre en full personvernkonsekvensvurdering av behandlingen. I tillegg til representanter for virksomheten, blir også leverandøren og lederen for det lokale eldrerådet invitert inn. Eldrerådet blir inkludert for å forsikre seg om at eldre pasienter vil kunne bruke innloggingsportalen.

Det blir også utarbeidet rutiner for roller og ansvar for fastlegene og sekretærene. Legekontoret har også en fysioterapeut som må ha en egendefinert rolle i modulen.

På bakgrunn av risikovurderingen og personvernkonsekvensvurderingen blir det iverksatt en rekke tiltak, blant annet retningslinjer for hva som kan sendes til pasientens postkasse, rutiner for opplæring av de ansatte og rutiner for avvikshåndtering.

Det inngås databehandleravtale med leverandøren. Til slutt lages det rutiner for hvordan pasientkommunikasjonen skal inkluderes i virksomhetens internkontroll.

Miniveikart for implementering av ny funksjonalitet eller ved anskaffelse av tredjepartsløsninger/applikasjoner:



3.2 Eksempler på rutiner

Krav:	Forslag til gjennomføring
Roller og ansvar	• Definere hvem som er dataansavarlig og eventuell databehandler • Hvem har eierskap til løsningen i virksomheten? • Hvem har det daglige ansvaret?

Gjennomføre risikovurdering	Se kapittel 2.2.1 og Veileder for rettigheter ved behandling av helse- og personopplysninger. Se kapittel 5 for eksempler på risikoscenarier
Innebygget personvern i løsningen	Løsningen må legge til rette for ivaretakelse av de registrertes rettigheter Stille krav om innebygget personvern og personvern som standardinnstilling Be leverandør gjøre rede for hvordan dette skal gjøres i løsningen
Gjennomføre DPIA	Se kapittel 2.2.2 Hvis mulig, ha med representant for bruker av løsningen i gjennomføringen
Etablere brukerrutiner	Se kapittel 2.7.
Etabler databehandleravtale	Benyttes det en tjeneste som leveres av en ekstern driftsleverandør skal det opprettes databehandleravtale mellom virksomheten og databehandler. Dette gjelder alle tjenester hvor det behandles helse- og personopplysninger. Se avtaleeksempel i Faktaark 10 – Bruk av databehandler (ekstern driftsleverandør) (på www.normen.no). Se også Vedlegg til Normen "Oversikt over Normens krav" med bl.a. følgende krav databehandler skal ivareta: - At løsningen oppfyller lovbestemte krav og kravene i Normen - Taushetsplikt for egne medarbeidere - Internkontroll, sikkerhetsrevisjoner og avviksbehandling - Ved terminering skal det foreligge en signert erklæring fra leverandøren om at alle data tilhørende virksomheten er tilbakelevert eller slettet til avtalt tid
Etabler internkontrolltiltak	Se kapittel 2.7.3 for eksempler på rutiner. For eksempler på rutiner og prosesser ved bruk av sosiale medier, se kapittel 3.2.

3.3 Krav til leverandører

Normen gjelder for enhver virksomhet som gjennom avtale med Norsk Helsenett har forpliktet seg til å følge den. Leverandører vil være forpliktet til å følge Normen dersom de har tilknytning til helsenettet, eller ved andre typer avtaler som databehandleravtale, tjeneste/driftsavtale, avtale om fjernsupport mm. Leverandører skal tilrettelegge for at dataansvarlig som tar i bruk leverandørens produkter og tjenester, kan oppfylle lovbestemte krav og kravene i Normen.

Hvilke av Normens krav som gjennom avtale gjelder for leverandører er avhengig av hva slags type leveranse det er snakk om, for eksempel:

- Databehandling, i form av for eksempel skytjenester eller driftstjenester
- Vedlikehold, for eksempel ved fysisk service eller fjernaksess
- Leveranse av løsninger og systemer

I de tilfellene hvor leverandøren ikke er forpliktet via avtale med Norsk Helsenett til å følge Normen, kan de allikevel pålegges å følge kravene via databehandleravtale eller annen avtale med virksomheten.

Tabellen nedenfor viser noen av Normens krav og mulig løsning for hvordan kravene kan ivaretas av leverandør for leveranse av digitale kommunikasjonsløsninger. Tabellen nedenfor inneholder eksempler på aktuelle krav og ikke alle kravene vil være relevante for alle leverandører.

For en fullstendig oversikt over alle systemkravene i Normen, bruk Vedlegg til Normens krav. For kommunikasjonsløsninger som brukes sammen med EPJ-system, se "Systemkrav i behandlingsrettet helseregister" i vedlegget for oversikt over samtlige systemkrav i Normen.

Eksempel på noen av kravene og mulige løsninger på kravet i praksis:

Relevante krav (for leverandører) i Normen	Utdyping av krav og mulige løsninger
4.1 Behandlingsgrunnlag	Dataansvarlig er ansvarlig for at samtykke fra pasienten/ brukeren er innhentet til å formidle helse- og personopplysninger elektronisk. Ved utvikling av nettportaler og applikasjoner for pasientkommunikasjon, bør leverandøren sørge for at det kan avgis samtykke elektronisk ved første gangs bruk av løsningen for pasientkommunikasjon. Samtykket bør skilles ut slik at den registrerte kan velge ut de de enkelte tjenestene som finnes i portalen/applikasjonen. For mer informasjon om samtykke, se Veileder for rettigheter ved behandling av helse- og personopplysninger.

4.2.3 Innsyn 4.2.4 Retting og sletting	Leverandøren må legge til rette for tekniske og organisatoriske tiltak slik at den registrerte kan få innfridd sine rettigheter. Dette innebærer at krav til innebygget personvern må hensyntas ved utvikling av løsninger. Løsningen må inneholde funksjonalitet som sørger for at dataansvarlig kan utføre retting og sletting av helse- og personopplysninger, eller at det finnes funksjonalitet som gjør at den registrerte kan rette egne opplysninger. Dersom løsningen behandler opplysninger som faller inn under dokumentasjonsplikten til helsepersonell, må ikke disse kunne endres eller slettes av den registrerte. Se også Veileder for rettigheter ved behandling av helse- og personopplysninger
5.4.4 Logging	Minimumskravene til logging følger av Normens krav 5.4.4. Dersom det behandles helse- og personopplysninger for andre formål enn ytelse av helsehjelp, for eksempel administrasjon av helsehjelp, skal kravene til logging fastsettes på bakgrunn av en risikovurdering.
5.7 Leverandørforhold og avtaler	Når leverandør utfører behandling av helse- og personopplysninger på vegne av dataansvarlig skal det inngås en databehandleravtale. Dersom leverandøren drifter løsninger for flere kunder skal den sørge for at det ikke opprettes registre som inneholder helse- og personopplysninger for flere kunder. Dette skal fremgå av databehandleravtalen. For leverandører av utstyr og/eller programvare som må ha adgang, til systemer som behandler helse- og personopplysninger, for vedlikehold, feilretting, oppdatering, ved hjelp av online tilkobling og/eller fysisk oppmøte skal det inngås en databehandleravtale. Det må sikres at det er inngått avtale som ivaretar taushetsplikten (enten ved inngåelse av databehandleravtale eller annen avtale). Drifter leverandør kun selve portalen/applikasjonen (grensesnittet mellom pasient/bruker og virksomhetens fagsystem) er det vesentlig å avtale at mellomlagringen må sikres og slettes i portalen etter at kommunikasjonen er gjennomført. Alternativt kan det benyttes PKI som sikrer kommunikasjonen mellom pasient/bruker og virksomhetens fagsystem. Mal for databehandleravtale med veileder finnes hos Direktoratet for e-helse. Utfylling av avtalen bør gjøres i samarbeid med dataansvarlig.

	Se også : - Faktaark 10 – bruk av databehandler - Faktaark 36 - Fjernaksess mellom leverandør og virksomhet
5.8.1 Avvikshåndtering	Leverandøren må ha rutiner for å oppdage, håndtere og melde brudd på personopplysningssikkerheten til dataansvarlig. Detaljerte krav til håndtering og melding av avvik kan detaljeres i en databehandleravtale.

4 Risikoscenarier

4.1 Generelle scenarier

Noen eksempler på scenarioer det kan være aktuelt å inkludere i en risikovurdering:

1. Pasient ser kommunikasjon til eller fra en annen pasient ved sending til feil mottaker
2. Brudd på taushetsplikten ved at informasjon sendes feil eller til flere enn tiltenkt.
3. Brudd på taushetsplikten ved at for mye informasjon sendes til pasienten
4. Andre enn pasienten har tilgang til utstyret som kommunikasjonen mottas til og får tilgang til pasientkommunikasjonen
5. Pasientkommunikasjon skjer i virksomheten uten lovlig rettsgrunnlag fordi informasjonen i kommunikasjonen brukes til andre formål enn opprinnelig bestemt (formålsutglidning)
6. Databehandleravtale er ikke opprettet med ekstern teknisk leverandør ved ekstern service på server og annet datautstyr som brukes i pasientkommunikasjon
7. Pasient / brukers innsynsrett lar seg ikke oppfylle fordi virksomheten ikke har kontroll / oversikt over hvor kommunikasjon lagres
8. Enheter som brukes til pasientkommunikasjon mistes, stjeles eller går tapt på annen måte
9. Ansatt sender informasjon til pasient ukryptert via e-post
10. Virksomheten har rutiner for kryptere dokumenter som inneholder helseopplysninger, men man glemmer å kryptere dokumentet og sender da epost uten kryptering.
11. Ansatte har ikke fått opplæring i hvordan digital pasientkommunikasjon skal skje i henhold til prosedyrer i virksomheten
12. Nettverk og PC/arbeidsstasjoner blir angrepet av datavirus eller ondsinnet kode
13. Stans i server med pasientkommunikasjon pga. tekniske problemer
14. Manglende tilgangskontroll til enheter eller PC/programvare som brukes til digital pasientkommunikasjon (personell uten tjenstlig behov har tilgang)

15. Oversikt over tildelte autorisasjoner for tilgang til systemer oppbevares mindre enn 5 år
16. Ansatt som slutter blir ikke fjernet som bruker i system med tilgang til journalsystem/pasientkommunikasjon
17. Ikke autorisert bruk og forsøk på uautorisert bruk registreres ikke som sikkerhetshendelser
18. Bygget hvor virksomheten holder til er utilgjengelig pga. brann, naturskade mv., og server med pasientkommunikasjon og sikkerhetskopier (backup) er midlertidig utilgjengelig eller går tapt (dersom fysisk lagring hos virksomheten)
19. Feiltolkning av informasjon i kommunikasjonen
20. Medarbeidere hos leverandøren får tilgang til helse- og personopplysninger.
21. Leverandøren er plassert utenfor EU/EØS
22. E-post: lytta på e-postlinja og "snapper opp" informasjonen i transitt.
23. E-post: Lage noen tilgjengelighetsscenarier: sender epost som ikke blir lest. Epostadresser som ikke blir brukt mer, byttet epost adresser, pasienter bytter navn.
24. Pasienten bytter telefonnummer eller sletter en app, har ikke på varsler.
25. Manglende lesebekreftelse på meldinger.
26. Overskuddsinformasjon slettes ikke, alt føres inn i journal uten at man tar stilling til om informasjonen er nødvendig.
27. Meldinger blir ikke slettet i kommunikasjonsapper.
28. Pasienten blir satt i en situasjon der man lagrer for mye informasjon uten at det er tiltenkt, eks i meldingsarkiv.
29. Opplysninger blir liggende i meldingsarkiv/logg/historikk og blir ikke slettet.
30. Meldinger blir lagret lokalt på enhetene til pasienten
31. SMS kan være avslørende i seg selv, for eksempel en SMS fra kreftregisteret eller "Du har fått ny time" fra Olafiaklinikken
32. Kriminelle aktører utnytter en kjent funksjonalitet og sender SMS eller e-post med skadelig programvare til pasienten som utgir seg for å være fra helsevirksomheten.
33. E-post/kommunikasjon blir utformet på en slik måte at pasienten tror meldingen er falsk og ignorerer den. (omvendt phishing).
34. Pasient har ikke Bank-ID eller annen sikker personlig ID.
35. Pasienten er i en sårbar gruppe og klarer ikke å innhente eller forstå informasjonen
36. Digitale angrep mot tjenester eksponert mot internett medfører brudd på konfidensialitet, integritet eller tilgjengelighet

4.2 Særskilte risikoer for sosiale medier

- Passord/innloggingsdetaljer til sosiale medier kommer på avveie slik at uvedkommende utgir seg for å være virksomheten og publiserer innhold
- Bruker på sosiale medier utgir seg for å være en annen i kontakt med helsetjenesten og får dermed nedtegnet informasjon i vedkommendes journal
- Det publiseres bilder/informasjon om pasienter uten samtykke
- Det publiseres bilder/informasjon om pårørende eller besøkende uten samtykke
- Det publiseres bilder/informasjon om ansatte uten samtykke

- Det publiseres innhold av andre enn helsepersonell på det sosiale mediet som inneholder sensitiv informasjon
- Det publiseres bilder/informasjon av pasienter som bor på hemmelig adresse
- Upassende innhold publisert av publikum blir ikke moderert eller slettet og blir liggende synlig for andre brukere
- Brukere i en sårbar situasjon tar kontakt med virksomheten når kontoen ikke er bemannet og publiserer sensitiv informasjon om seg selv.
- Brukere tar screenshots av innhold som ikke skal være der og sprer dette
- Helsepersonell kommuniserer med pasienter/pårørende i chatfunksjon og utleverer helseopplysninger om pasient/bruker i kommunikasjon på sosiale medier
- Publikum får generert målrettet reklame med misvisende innhold.
- Brukervilkår og tjenestevilkår endres uten at virksomheten får varsel om det
- Innhold blir sensurert eller slettet av tjenesteleverandøren, slik at integriteten i informasjonen blir påvirket
- Innhold blir slettet fra brukerkontoen, men slettes ikke av leverandøren sine servere
- Manglende retningslinjer for dokumentasjon medfører avvik mellom det pasienten skriver og det som blir nedtegnet.
- Lukkende grupper for ruspasienter brukes til andre formål
- Lukkede grupper blir ikke konfigurert på riktig måte, slik at medlemmene i gruppene er synlige for alle
- Lukkede grupper gis navn som avslører en pasientgruppe
- Lukkede grupper kan være synlige via søkemotorer
- Nettroll kan publisere skadelig, feilaktig eller plagsomt innhold

5 Vedlegg

5.1 Eksempler på innhold i elektronisk pasientkommunikasjon

Dette vedlegget inneholder eksempler på formuleringer av innhold i SMS og e-post, men kan også benyttes ved bruk av andre kommunikasjonsverktøy. Virksomheten som benytter løsningen er ansvarlig for og skal påse at krav til informasjonssikkerhet ivaretas. Formuleringene kan benyttes i andre kanaler enn SMS og e-post der de passer.

Den samlede informasjonen i kommunikasjonen må vurderes ut fra om innholdet totalt sett kan medføre brudd på taushetsplikten.

5.1.1 Eksempler på innhold i SMS:

Eksempler på informasjon som **kan** sendes som SMS

- Navn, helst kun fornavn
- Fødselsdato, kun dato, måned og år

- Bestilling av time
- Bekreftelse på timeavtale (”..minner om timeavtale hos oss tir. 5. jan kl. 1430. Mvh. <Normbakken Legesenter>”)
- Aksept av timeavtale (svar tilbake til avsender at avtalen er OK – Ja/Nei)
- Endring av timeavtale (Time 5. jan kl 1200 utgår. Du er satt opp med ny time 18. januar kl 1700. Bekreft om foreslått tidspunkt passer – Ja/Nei)
- Forespørsel om blodgiving
- Aksept av blodgiving (Ja/Nei)
- Bekreftelse på at en resept er klar til henting (”Resepten din er ferdig og klar for henting”)
- Engangspassord for pålogging til kommunikasjonsløsninger som inneholder helseopplysninger
- Varsling om nye meldinger i andre systemer
- Annet som er relatert til praktiske forhold vedr. kontakten mellom helsetjenestetilbyder og pasienten/brukeren, og som ikke inneholder sensitive personopplysninger (”...vi har flyttet til...”)
- Hvis det ikke kan eller skal sendes svar på SMS skal det opplyses om det i meldingen som sendes til pasienten/brukeren, f. eks kan meldingen utvides med: ”Du kan ikke sende svar på denne SMS”

Hver enkelt virksomhet må vurdere om navn på avdelinger eller oppmøtesteder som er tenkt brukt i SMS-varsel er av en slik karakter at det kan avledes opplysninger om diagnose eller helseforhold. For eksempel skal ikke avdelingsnavn som ”... psykiatrisk poliklinikk...”, ”...gynekologisk avdeling...” benyttes.

Eksempler på informasjon som **ikke kan** sendes som SMS

- Helseopplysninger. Dette gjelder for eksempel diagnose i form av kode eller tekst som viser pasienten/brukerens helsetilstand.
- Reseptinformasjon. Dette gjelder for eksempel innhold i eller forordning av legemiddel
- Avdelingsnavn (som kan knyttes til diagnose eller helseforhold. Unngå for eksempel ”...psykiatrisk poliklinikk...”, ”...gynekologisk avdeling...”)

Eksempler på informasjon som **ikke bør** sendes som SMS

- Fødselsnummer (11 siffer)[6]
- Telefonnummer til avsender (slik at det ikke er mulig å identifisere avsender/avdeling med navn som kan angi helseforhold eller diagnose).

[6] Ifølge Datatilsynet kan fødselsnummer kan i enkelte tilfeller kommuniseres over SMS, fordi denne kommunikasjonsformen har en viss informasjonssikkerhet. For mer informasjon se Datatilsynets nettsider

5.1.2 Eksempler på innhold i e-post

Virksomheten skal etablere tiltak som sikrer at helse- og personopplysninger ikke sendes eller tilgjengeliggjøre ved hjelp av ukryptert/usikker e-post. Dette betyr at det må etableres rutiner for kryptering av e-post dersom det skal sendes helseopplysninger eller annen sensitiv informasjon.

Dersom ukrypterte kanaler brukes for å kommunisere med pasient, må virksomheten:

- Ha rutiner som sikrer at e-poster ikke inneholder identifiserbare helseopplysninger

– Etablere logging for å kontrollere at rutiner ikke brytes

– I alle tilfeller, vurdere om den samlede informasjonen kan medføre brudd på taushetsplikten. Se også kapittel 2.3.2 om taushetsplikt.

Eksempler på informasjon som **kan** sendes i ordinær e-post:

- Navn, helst kun fornavn
- Fødselsdato, kun dato, måned og år
- Bestilling av time
- Bekreftelse på timeavtale (”..minner om timeavtale hos oss tir. 5. jan kl. 1430. Mvh <navn>”)
- Aksept av timeavtale (svar tilbake til avsender at avtalen er OK – Ja/Nei)
- Endring av timeavtale (Time 5. jan kl. 1200 utgår. Du er satt opp med ny time 18. januar kl
  1700. Bekreft om foreslått tidspunkt passer – Ja/Nei)
- Forespørsel om blodgiving
- Aksept av blodgiving (Ja/Nei)
- Bekreftelse på at en resept er klar til henting (”Resepten din er ferdig og klar for henting”)
- Varsling om nye meldinger i andre systemer
- Annet som er relatert til praktiske forhold vedr. kontakten mellom helsetjenestetilbyder og pasienten/brukeren, og som ikke inneholder sensitive personopplysninger (”...vi har flyttet til...”)
- Hvis det ikke kan eller skal sendes svar på e-post, skal det opplyses om det i e-posten som sendes til pasienten/brukeren, f.eks kan meldingen utvides med: "Du kan ikke sende svar på denne e-posten".

Eksempler på informasjon som **ikke kan** sendes i ordinær e-post:

- Fødselsnummer (11 siffer)
- Helseopplysninger. For eksempel diagnose i form av kode eller tekst som viser pasienten/brukerens helsetilstand
- Reseptinformasjon. For eksempel innhold i eller forordning av legemiddel
- Avdelingsnavn (som kan knyttes til diagnose eller helseforhold. Unngå for eksempel ”...psykiatrisk poliklinikk...”, ”...gynekologisk avdeling...”)

Eksempler på informasjon som **ikke bør** sendes i e-post

- Telefonnummer til avsender (slik at det ikke er mulig å identifisere avsender/avdeling med navn, som kan angi helseforhold eller diagnose)

Besøksadresse
Verkstedveien 1
0277 Oslo

Kontakt
postmottak@ehelse.no