Direktoratet for e-helse

Veileder for kvalitetssikring av ikke-medisinske helseapper

HITS 1250 *høringsutkast* 2023

Publikasjonens tittel:
Veileder for kvalitetssikring av ikke-medisinske helseapper

Rapportnummer
HITS 1250 høringsutkast 2023

Utgitt:
06/2023

Utgitt av:
Direktoratet for e-helse

Publikasjonen kan lastes ned på:

www.ehelse.no

Innhold

1 Innledning

1.1 Bakgrunn

Dette dokumentet er et evalueringsrammeverk som er basert på arbeidet gjennomført i prosjektet Tryggere helseapper, eid og ledet av Helsedirektoratet. Prosjektet varte fra oktober 2021 til november 2022 og Norsk helsenett og Direktoratet for e-helse bidro i prosjektet.

I prosjektet ble det utarbeidet et kunnskapsgrunnlag som viste at helsetjenesten ønsket å øke bruken av helseapper, men at det også var et behov for å kvalitetssikre helseappene.

Prosjektet piloterte våren 2022 et evalueringsrammeverk basert på SN-CEN ISO/TS 82304-2:2021 «Apper for helse og velvære – Kvalitet og pålitelighet». Spesifikasjonen er internasjonal og gjelder både for apper som regnes som medisinsk utstyr og ikke-medisinske apper. Den er omfattende og stiller krav til dokumentert helsenytte, brukskvalitet, personvern, databehandling, informasjonssikkerhet og interoperabilitet. Spesifikasjonen inneholder en sjekkliste med et scoringssystem som kan brukes til å gi appen et kvalitetsmerke, en form for etikett som viser hvor godt appen tilfredsstiller de ulike kravene.

Evalueringsrammeverket ble laget for å dekke behovet for kvalitetssikring av apper som **ikke** kategoriseres som medisinsk utstyr. Merk at det gjelder egne krav for apper og andre digitale verktøy som omfattes av regelverk for medisinsk utstyr. Se mer hos Legemiddelverket.

Målet var at evalueringsrammeverket skulle kunne brukes av helsemyndighetene til å kvalitetssikre slike apper, slik at helsetjenesten og innbyggerne vet at de er gode og trygge å bruke. Det er hver kommune, virksomhet eller hvert helseforetak som anskaffer eller gjør tilgjengelig helseapper selv, som har ansvaret for å vurdere behov, nytte og sikkerhet.

Det finnes mange apper som kan gi helsenytte for den enkelte, uten å gå under definisjonen for medisinsk utstyr. Eksempler på dette er treningsapper, kalendere, verktøy for læring og mestring osv. Det er viktig at også slike apper holder en god kvalitet, men at kravene kan være noe mindre omfattende enn det ISO-dokumentet legger opp til.

Spørsmålene og evalueringskriteriene som ble lagt inn i rammeverket var i prinsippet en syntese av kravene i spesifikasjonen fra ISO, tilpasset norske forhold. Kravene i evalueringsrammeverket representerer et sett av minimumskrav som samsvarer med kravene i ISO-dokumentet, men som er mindre omfattende og skrevet på norsk. I tillegg blir det vist til krav knyttet til å gjøre appene tilgjengelig for innbyggere gjennom Helsenorge, se kap. 4.

Evalueringsrammeverket ble pilottestet av fem appleverandører i prosjektet, og oppdatert basert på erfaringene fra uttestingen, se Tryggere helseapper. Videre har mappingen mellom kravene i evalueringsrammeverket og ISO-spesifikasjonen blitt lagt inn, slik at det er enkelt å se hvilke krav som er felles (dette dokumentet). Ordlyden fra enkelte krav i evalueringsrammeverket har blitt justert slik at de samsvarer bedre med ISO-spesifikasjon.

1.2 Begrepsavklaringer

1.2.1 Helseapp

Veilederen bruker begrepene “app” og “helseapp”, som samlebegrep for mange digitale løsninger og verktøy, dvs. software, som kan brukes av innbyggere. Dette omfatter både frittstående mobilapper, web-apper, nettsider med informasjon og veiledningsmateriell og samvalgsverktøy. Dette gjelder kun helseapper som ikke er kategorisert som medisinsk

Kommentert [GV1]: Bakgrunnen oppfattes som litt lang og tungt formulert.

Forslag til endring:
- Korte ned og forenkle innholdet.
- Legge inn mer allmenngyldige forhold innledningsvis i bakgrunnen, som f.eks "Apper og digitale helseverktøy kan bidra til å forebygge, lindre og mestre en lang rekke diagnoser og helseplager, og gjøre oppfølgingen fra helsetjenesten bedre. Både for helsepersonell og folk flest er det vanskelig å skille gode og trygge helseapper fra de mindre gode eller til og med skadelige. Veilederen tar deg gjennom kriterier og rammeverk som bør følges for å sikre at man utvikler og tar i bruk helseapper med nødvendig kvalitet."

Kommentert [GV2]: Dette dokumentet inneholder en veldig forenklet versjon av det rammeverket som er blitt pilotttestet.

Forslag til endring:
Teksten bør justeres slik at den gir en korrekt fremstilling.

Kommentert [CS3]: Se innspill til dette i eget dokument.

utstyr. Definisjonen på medisinsk utstyr kan leses på Statens legemiddelverk sine sider, Medisinsk utstyr fra A-Å - Legemiddelverket.

2 Bruksområde og formål

Bruksområdet for veilederen er helseapper og digitale helseverktøy som **ikke** er medisinsk utstyr. Avgjørelsen om noe er et medisinsk utstyr skal baseres på produsentens formål med produktet, se Statens legemiddelverk om klassifisering. Veilederen gir oversikt over krav, regler og prosedyrer som minimum bør ivaretas ved utvikling, anskaffelser og bruk av slike apper. Veilederen beskriver kriterier og krav til helsenytte, brukskvalitet, universell utforming, personvern og informasjonssikkerhet, i tillegg viser veilederen til krav som må følges hvis en app skal gjøres tilgjengelig via Helsenorge. Det er ikke et krav i veilederen at helseapper skal gjøres tilgjengelig via Helsenorge.

Formålet med veilederen er å øke kvaliteten på helseapper som ikke regnes som medisinsk utstyr i Norge, ved at disse minimumskriteriene blir gjort lett tilgjengelig, på norsk.

Veilederen er relevant for virksomheter som bestiller, anskaffer, utvikler og tilgjengeliggjør helseapper. Per i dag vil den kunne brukes som en form for sjekkliste, dvs. den er ikke del av en godkjenningsordning for helseapper i det offentlige.

Virksomheter som vurderer å ta i bruk en helseapp kan bruke veilederen

- til å vurdere om appen er trygg og egnet for formålet.
- som del av kravspesifikasjon.
- til å utforme evalueringskriterier ved anbudskonkurranser.

For utviklere/leverandører vil veilederen ha nytteverdi

- som kravspesifikasjon som må være oppfylt for at en helseapp skal kunne vurderes som et tilbud i den offentlige helsetjenesten.
- som en sjekkliste i en tidlig fase av konsept- og tjenesteutviklingen.
- som et verktøy underveis i utviklingen av en app.

Norsk helsenett kan bruke kriteriene når apper skal gjøres tilgjengelig via Helsenorge.

2.1 Ønsket effekt av å normere veilederen

Direktoratet for e-helse publiserer dette dokumentet som et normerende produkt for å

- gjøre kvalitetskriterier lett tilgjengelige på norsk for leverandører, virksomheter m.m.
    -

Kommentert [CS4]: Kan man her også få frem fordelene med å tilgjengeliggjøre via Helsenorge, ref oversiktsprinsippet? "*Veilederen er generell på tvers av alle bruksområder den offentlige helsetjenesten har for apper. Det er ikke et krav i veilederen at helseapper skal publiseres på Helsenorge, men det er mange fordeler med det. Om det skal gjøres eller ikke blir ivaretatt av prinsippene for koblinger mellom Helsenorge og andre løsninger i markedet. En av fordelene med å gjøre helseappen tilgjengelig på Helsenorge er gjøre det enklere for helsepersonell og innbyggere å tildele og finne Helseapper som er vurdert som trygge. En annen fordel er at innbygger vil ha en samlet oversikt over alle sine helseapper og lett finne dem igjen i sin oversikt.*"

Kommentert [GV5]: Formålet er bredere enn det som er beskrevet.

Forslag til endring:
Legge til følgende setning: "Veilederen skal gjøre det lettere for kommuner, helseforetak og andre offentlige virksomheter å anskaffe, ta i bruk og/eller anbefale helseapper til innbyggere og pasienter"

Kommentert [CS6]: Se innspill til dette i eget dokument.

Kommentert [CS7]: NHN er nevnt eksplisitt som aktuell bruker av veilederen når verktøy skal legges i verktøykatalogen. NHN har ikke – og skal ikke ha - ansvar for kvalitetssikringen av apper som offentlig bestiller ønsker å legge inn i verktøykatalogen, og har i tillegg egne krav som stilles til appene som ønskes tilgjengeliggjort via Helsenorge. Det fremstår også unaturlig at én aktør er nevnt direkte og det anbefales at dette fjernes. Helsemyndighetene er for øvrig ikke nevnt som bruker av veilederen, men er i dag den aktøren som anskaffer flest helseapper som skal tilgjengeliggjøres for hele befolkningen. Det bør vurderes om de skal nevnes eksplisitt som aktørgruppe eller om de omfattes av eksisterende ordlyd " virksomhet som vurderer å ta i bruk en helseapp" i veilederen.

3 Kriterier

Dette kapittelet beskriver krav om informasjon om leverandør og helseapp, helsenytte, brukskvalitet, universell utforming, personvern og databehandling.

Kravene for helseapper og helseverktøy er vist i tabeller. Noen av kravene er relatert til krav i SN-CEN ISO/TS 82304-2:2021 «Apper for helse og velvære – Kvalitet og pålitelighet». Der dette er tilfelle, er mappingen vist i tabellene. Det er ikke alltid én-til-én mapping mellom krav i denne veilederen og i spesifikasjonen fra ISO, og derfor er det angitt flere referanser til ISO-spesifikasjonen for noen krav.

3.1 Informasjon om leverandør og helseapp

Nr.	Spørsmål/opplysning	ISO/TS 82304-2
1	**Navn på virksomhet** Med virksomhet menes det juridiske eller fysiske selskapet eller virksomheten som gjør appen tilgjengelig og er ansvarlig i henhold til gjeldende lovgivning. I noen tilfeller vil det være app-utgiver som står som virksomhet.	5.1.2.1
2	**Kontaktinformasjon til personen som er autorisert til å representere virksomheten.** Angi navn, rolle, telefon og e-post. Ettersom enkeltpersoner kan endre roller, er en rollebasert e-postadresse anbefalt.	5.1.2.2
3	**Navn på helseapp** Navnet som benyttes i markedsføring.	5.1.1.2
4	**Lenker til Appstore/Google Play/andre nettsteder der appen presenteres.**	
5	**Formål med appen** • Hva vil brukerne oppnå ved å benytte appen? • Det skal være enkelt for brukerne å oppfatte hva de kan oppnå om de benytter appen. • Beskrivelsen skal samsvare med tekst i App store, Google Play og eventuelt andre steder. • Antatte effekter ved bruk av helseappen skal kunne dokumenteres. Dokumentasjon kan være forklaring i tekst, supplert med skjermbilder, ev. animasjon/film som illustrerer hva brukeren møter.	5.2.1.3 5.2.1.4

Nr.	Spørsmål/opplysning	ISO/TS 82304-2
6	**Målgruppe for appen** • Hvem er appen utviklet for og hvilke(n) helseutfordring(er) og/eller helsebehov er appen for? Herunder kjønn, alder, og andre egenskaper som definerer målgruppen(e). • Beskrivelsen skal samsvare med tekst i App store, Google Play og eventuelt andre steder.	5.2.1.1
7	**Hvilken kategori eller kategorier hører appen under?** 1. Kommunikasjon/dialog/system/samhandling/støtte til forløp og oppfølging. Apper og helseverktøy som forbedrer dialog og oppfølging for helsepersonell og pasient. Kategorien inkluderer for eksempel elektroniske forskrivningssystemer, timebestilling, dialogsystemer, meldingsutveksling og videoløsninger. 2. Informasjon Appen inneholder informasjon om forebygging, sykdomsspesifikke tiltak, egenomsorg og lignende. 3. Monitorering/kartlegging Appen legger til rette for at brukeren kan registrere og følge med på symptomer, utvikling, livsstil-parametere og eventuelt dele disse med behandlere. Eksempler: Hodepinedagbok, smerteregistrering og registrering av fysisk aktivitet. 4. Forebygging/mestring gjennom atferdspåvirkning/motivasjonsteknikker Apper som skal føre til endring i atferd. Dette inkluderer endring av tankemønstre gjennom informasjon, teknikker og øvelser. Eksempler: Røykeslutt, fysisk aktivitet.	5.2.1.4

3.2 Brukskvalitet

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
8	**Har personer med relevant helsefaglig kompetanse vært involvert i utvikling av appen?**	5.2.1.6

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
	Beskriv hvem som har vært involvert inkl. relevant utdanning og yrkeserfaring, hyppighet, hvordan de har deltatt og hvilken påvirkning de har hatt på prosessen.	
9	**Har pasienter/brukere/representanter for målgruppen deltatt i utvikling av produktet/appen?** Beskriv hvem som har vært involvert inkl. fra hvilke organisasjoner, hyppighet, hvordan de har deltatt og hvilken påvirkning de har hatt på prosessen.	5.3.2.2
10	**Er designet av helseappen basert på en eksplisitt forståelse av brukernes behov, oppgaver og kontekst?**	5.3.2.1
11	**Er designet utviklet og justert med en brukersentrert tilnærming?**	5.3.2.3
12	**Er det implementert tiltak/justeringer for å redusere muligheten for brukerfeil?**	5.3.2.4
13	**Får brukere tilstrekkelig instruksjon for å benytte appen?**	5.3.2.5
14	**Er det etablert et tilstrekkelig brukerstøttesystem?**	5.3.2.7
15	**Benyttes brukerdata systematisk for å forbedre funksjonaliteten?**	5.3.2.8
16	**Foreligger det en plan for løpende brukertesting og videreutvikling?**	5.3.2.8

Eksempler på egnet dokumentasjon av brukskvalitet:

- Rapporter som dokumenterer brukerevalueringer og -testing, konsultasjoner med ekspertpaneler og annen relevant innsikt benyttet til å kvalitetssikre appen og sikre at brukerne kan benytte den.
- Rapport fra et uavhengig test/evalueringsmiljø som oppsummerer brukernes opplevelse av nytte. Hvis appen er rettet mot et visst alderssegment eller til personer med et bestemt helseproblem eller funksjonshemming, må personer som har disse helseproblemene/funksjonshemmingene være deltakere i brukertestene.

3.3 Helsefordeler

Når helsetjenesten tar i bruk nye metoder, medikamenter og tjenester stilles det strenge krav til at helseeffekter og eventuelle bivirkninger er nøye vurdert og dokumentert. Dette kravet gjelder også apper. Noen apper kan inneholde pedagogiske og engasjerende presentasjoner av informasjon som man ellers ville finne i bokform eller på nettsider. Andre apper gjør det mulig å registrere fysisk aktivitet og kan inneholde motivasjonselementer.

Noen apper er enkle og har lav risiko for å forårsake skade eller uheldige bieffekter, mens andre kan føre til livstruende situasjoner dersom de svikter eller har feil eller mangler. Dette spennet bør reflekteres i hvor strenge krav man stiller til testing.

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
17	**Hvilken nytte/helsefordeler brukerne kan forvente ved å bruke appen?** Beskrivelsen skal være i overensstemmelse med øvrige beskrivelser av appen og markedsføringsmateriell.	5.2.4.1
18	**Finnes det støtte for at appen holder det den lover?** Legg ved eventuell referanse til forskning, tester osv. Eksempler på dokumentasjon: • Kunnskapsoppsummeringer • Publiserte og fagfellevurderte studier • Evalueringsrapporter og/eller vurderinger fra uavhengig og anerkjente fagmiljø • Tidligere studier av metoden som benyttes i appen. For eksempel kognitiv terapi, validerte algoritmer og eksempler på andre apper som bruker metoden • Rapporter fra brukerpaneler, brukertester og lignende	5.2.4.5
19	**Er det vurdert hvilken helserisiko/utilsiktede effekter appen kan ha for brukeren?** Eksempel på dokumentasjon: Risikoanalyse.	5.2.2.1
20	**Finnes det vurderinger av samfunnseffekter av appen?** Hvis det er gjort en utredning av samfunnseffekter: Beskriv om appen kan forbedre og/eller effektivisere pasientbehandling, og om den eventuelt kan generere merarbeid.	5.2.5.1

3.4 Universell utforming

Offentlige og private virksomheter med tjenester rettet mot allmennheten har plikt til å følge krav om universell utforming. Med universell utforming menes utforming eller tilrettelegging av et tilbud/tjeneste, slik at den kan benyttes av flest mulig, uavhengig av alder, funksjonsnivå og utdanningsnivå.

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2

Kommentert [CS8]: Det er bedre å referere til en harmonisert standard (TS er en Teknisk Spesifikasjon og rangerer lavere enn en standard. Bør endres til NKOM-EN 301 549 som er harmonisert – dvs. laget på mandat fra EU og dermed lovfestet, også i Norge.

21	**Er appen utviklet i henhold til forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger?**	
22	**Er appen i henhold til WCAG 2.1 nivå AA eller AAA?**	5.3.1.1
23	**Er WCAG 2.1 AA-kompatible tiltak etablert for å sikre at alle tilsiktede brukere kan oppfatte all relevant informasjon, og navigere etter hensikten?**	5.3.1.1.1

For dokumentasjon av spørsmålene om universell utforming, gå til siden Sjekk nettstedet ditt selv på uutilsynet.no.

3.5 Personvern og databehandling

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
24	**Er det etablert en behandlingsoversikt med forklaring på hvilke personopplysninger som samles inn til hvilket formål og på hvilke systemer?** Inneholder behandlingsoversikten rettslig grunnlag for hver behandling? Se Datatilsynets veileder om protokoll over behandlingsaktiviteter.	5.4.1.1.3
25	**Har virksomheten utarbeidet en personvernerklæring?** Blir den oppdatert ved behov? Se Datatilsynets veileder om Informasjon og åpenhet: Hva skal virksomheten gi informasjon om. Legg ved lenke til personvernerklæringen.	
26	**Er personvernerklæringen lett tilgjengelig for brukeren?**	5.4.1.1.4
27	**Er krav om formålsbegrensing og dataminimering ivaretatt?**	5.4.1.1.2
28	**Er personvernerklæringen skrevet slik at innholdet er forståelig og tydelig for målgruppen?** Se Datatilsynets veileder om Informasjon og åpenhet: Hva skal virksomheten gi informasjon om.	5.4.1.1.4.1
29	**Har virksomheten en dedikert person som ansvarlig for personvern (personvernombud)?** Se Datatilsynets veileder om virksomhetens plikter: personvernombud.	5.4.1.1.7

Kommentert [CS9]: Innspill - det bør heller henvises til seneste utgave av WCAG. Nå i august kom f.eks. WCAG 2.2 versjonen. WCAG er delt i nivå A, AA og AAA (som batterier). A er must have, AA er should have og AAA er nice to have. I Norge og EU er det A og AA nivåene som er lovfestet, derfor mener jeg det ikke bør stå AAA i veilederen. Forslag: Er appen i henhold til kravene i seneste utgave av WCAG, nivå AA?

Kommentert [CS10]: Forslag til endring i tråd med kommentarer over: bli Er tiltak etablert i henhold til seneste versjon av WCAG nivå AA?

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
30	**Legg ved en liste over alle underleverandører og tredjeparter som appen benytter.**	
31	**Er forbrukerrettighetene som er definert i GDPR enkelt og godt forklart for brukeren?**	5.4.1.1.4.1 5.4.2.11
32	**Er det enkelt for brukeren å be om ulike rettigheter?** Som retten til • sletting • endring • innsyn • dataportabilitet • å trekke samtykke • å kunne be om eksporterte data	5.4.1.1.3 5.4.1.1.4
33	**Dersom appen kan brukes av barn, foreligger det en egen avtale og punkt i personvernerklæringen?**	
34	**Hvis det er behov for samtykke av personvernerklæringen for et barn, er den tilrettelagt slik at samtykke kan utføres av foresatte?**	
35	**Er aldersbegrensninger av de tiltenkte brukerne eller pasienter under omsorg tydeliggjort for kunder og brukere?**	5.2.1.2
36	**Er appen passende med tanke på alder av brukerne?**	5.3.1.2 5.2.1.2
37	**Er det laget en personvernkonsekvensvurdering for appen?**	
38	**Er det signert databehandleravtaler mellom alle databehandlere og behandlingsansvarlige?** • Er disse tydelige og gjelder for behandling og avklart formål?	5.4.1.1.5

Kommentert [EM11]: "Registrerte" er ikke alltid forståelig, men "forbruker" gir kanskje feil assosiasjoner? Forbrukere har en rekke rettigheter, men rettighetene det er snakk om her er de registrertes.

Kommentert [EM12]: Ville det vært en effektiv forenkling å knytte krav 31 og 32 sammen, og ikke eksemplifisere, men å lenke til Datatilsynets veiledning? https://www.datatilsynet.no/rettigheter-og-plikter/den-registrertes-rettigheter/

Kommentert [EM13]: Hva slags egen avtale er det snakk om?

Kommentert [EM14]: Man samtykker til en behandling av personopplysninger

Kommentert [EM15]: Vil det alltid være slik at det er nødvendig med foresattes samtykke i denne sammenhengen?

Kommentert [EM16]: Passende på hvilken måte? Dette er kapittelet om personvern - er det snakk om tilpasset informasjon om behandling av personopplysninger bør det spesifiseres.

3.6 Informasjonssikkerhet

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
39	**Er det etablert et styringssystem for informasjonssikkerhet i virksomheten, f.eks. iht. ISO 27001/2 eller tilsvarende? Sikrer man at også underleverandører som tilbyr tjenester i tilknytning til produktet/appen har et slikt styringssystem?** • Er styringssystemet dokumentert og hvor? • Hvordan sikrer man at styringssystemet er operasjonalisert i organisasjonen?	5.4.2.1
40	**Er livssyklusen til appen og underliggende infrastruktur håndtert og dokumentert ved at:** • Dokumentasjon er tilgjengelig for eksisterende underliggende infrastruktur og denne holdes oppdatert? • Appen kan håndtere uforutsette ytelsesbehov eller økning av ytelse over tid? • Tekniske og administrative aktiviteter er etablert knyttet til etablering, vedlikehold og endring av appens konfigurasjon over produktets livssyklus? • Det gjennomføres jevnlig tester/validering av appen og underliggende infrastruktur for å sikre at forventet tjeneste kan leveres. Testresultater dokumenteres og kan monitoreres over tid.	5.5.1.1-8
41	**Er det fulgt en prosess for sikker utvikling av appen?** • Hvordan gjennomføres trusselvurderinger / tekniske sikkerhetsvurderinger ved utvikling og forvaltning av appen? ○ Dekker disse vurderingene underliggende infrastruktur eller underleverandører, og spesielt integrasjon ved disse? • Ved funn av sikkerhetsutfordringer i utvikling; hvordan følges disse opp i utviklingsprosessen/forvaltningsprosessen? • Vurderes dataminimering som del av prosessen slik at minst mulig data lagres/benyttes av appen? • Hvordan følges prinsippene om "Secure by design" og "Privacy by design" som sikrer sikkerhet og personvern i alle deler av utviklingen?	5.4.2.3

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
	• Hvordan håndteres sikkerhet ved bruk av tredjepartskomponenter/biblioteker? • Er sikkerhetstesting integrert i utviklingsprosessen? • Sikres det at tiltakene dekker de mest vanlige sikkerhetsutfordringene basert på en kjent standard slik som f.eks. OWASP TOP 10 eller andre standarder?	
42	**Hvordan er kildekoden beskyttet i utvikling og ved bruk?** • Hvordan er tilgang til kildekode og konfigurasjon beskyttet for å unngå utilsiktet eller uønsket endring av kildekoden? • Eksisterer det rutiner og prosesser for å sikre at endringer i koden verifiseres før det publiseres til produksjon, f.eks. ved krav til QA av annen utvikler? • Er appen beskyttet slik at det er vanskelig for andre apper å endre kode under kjøring eller påvirke appen på andre måter?	5.4.2.5

43	**Hvordan sikres sikker autentisering, autorisering og håndtering av sesjoner i appen?**
	• Brukes en standardtjeneste som f.eks. ID-porten for autentisering eller benyttes det egenopprettede brukere?
	  ○ Hvordan er sikkerhetsnivået på autentisering av bruker vurdert opp mot behovet i appen (typen informasjon som behandles)?
	• Ved bruk av egenopprettede brukere/autentisering; Beskriv hvordan dette er konfigurert og håndtert.
	• Hvordan håndteres sesjoner på en sikker måte?
	  ○ Vil en utlogging i appen alltid kreve ny innlogging og hvordan håndteres evt. Single sign-on (SSO) og single log-out (SLO)?
	  ○ Kan en bruker avslutte en sesjon / logge ut fra en annen enhet dersom f.eks. telefonen mistes eller stjeles?
		5.4.2.7

44	**Hvordan håndteres person- eller sensitive opplysninger ved behandling i appen?** • Hvordan beskyttes og krypteres data ved ev. lokal lagring? • Krypteres alltid data ved overføring og hvordan håndteres dette?	5.4.2.4 5.4.2.5 5.4.2.7 5.4.2.8

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
	• Benyttes kjente kryptografibiblioteker i kode eller er det egenutviklet? • Hvordan håndteres ev. krypteringsnøkler sikkert i app? • Ved overføring av data; hvordan verifiseres det at avsender og mottaker er korrekt?	
45	**Hvordan er appen sikkerhets- og penetrasjonstestet?** • Hvilke sikkerhets- og penetrasjonstester er utført av interne og/eller eksterne, og er resultatet dokumentert og tilgjengelig? • Gjøres testing iht. standarder for dette og/eller testes det for de mest kjente sårbarhetene i appen som utvikles? • Gjennomføres slike tester regelmessig og ved større endringer?	5.4.2.10
46	**Har det blitt gjennomført en sikkerhetsvurdering/gjennomgang av appen?** (Dokumentert ved f.eks. en risiko og sårbarhetsvurdering (RoS) som er tilgjengelig for innsyn) • Dekker vurderingen(e) underliggende infrastruktur? • Dekker vurderingen(e) appen og tilhørende avhengigheter? • Dekker vurderingen(e) håndtering og beskyttelse av innsamlet informasjon, inkludert personinformasjon og sensitiv informasjon? • Dekker vurderingen prosesser for forvaltning og drift av appen? • Finnes det restrisiko og hvordan er disse håndtert? • Finnes det rutiner og prosesser for å holde slike vurderinger oppdatert?	5.4.2.2
47	**Er det etablert prosesser for å håndtere sårbarheter når appen er tilgjengelig og i bruk?** • Hvordan testes appen jevnlig for å oppdage sårbarheter? • Finnes det dokumenterte prosesser for å oppdage og håndtere sikkerhetsutfordringer løpende og håndtere dette?	5.5.1.8
48	**Er en beskrivelse av informasjonssikkerheten og prosessen for å ivareta denne tilgjengelig for brukerne?** • Dekker den hele prosessen for å ivareta sikkerhet?	5.4.2.11

Nr.	Spørsmål/Opplysning	ISO/TS 82304-2
	• Dokumenterer den sikkerhetsstandarder som er i bruk og prosessen med å ivareta sikkerheten i appen? • Er den enkel å finne for en bruker av appen?	

4 Plattformspesifikke krav

4.1 Publisering av helseapper på Helsenorge

Hvis det er ønske om å publisere helseapper på Helsenorge må gitte tilleggskrav oppfylles. Disse finnes på siden Krav: Klassifisering og godkjenning av digitale verktøy hos Norsk helsenett.

Helseapper som gjøres tilgjengelig på Helsenorge vil inngå i innbyggers offentlige helse- og omsorgstilbud. Aktører som inngår i det offentlige helse- og omsorgstilbudet, kan avtale med Norsk helsenett at appen gjøres tilgjengelig.

- Per i dag er Helsenorge regulert for bruk av aktører innen det offentlige helsevesenet jf. forskrift om pasientjournal. Dette vil si at bestillingen må komme fra en helseaktør som inngår i det offentlige helse- og omsorgstilbudet.
- Apper som skal integreres med Helsenorge bør i tillegg følge Prinsipper for innbyggertjenester - kobling mellom Helsenorge og andre tjenester i markedet

Apper som benyttes som del av det offentlige helsetilbudet skal oppfylle krav til å samspille med andre løsninger som benyttes i sektoren. Hvilke krav som gjelder, er avhengig av funksjonaliteten i løsningene.

Som en forberedelse til publisering på Helsenorge, bør følgende spørsmål besvares:

Nr.	Spørsmål/Opplysning
49	**Skal appen være tilgjenglig for innbyggere som en del av det offentlige helsetilbudet?** • Kan den gjøres tilgjengelig i ulike kontekster som Google Play og Appstore, og i Verktøykatalogen på Helsenorge?
50	**Skal appen formidles til enkeltpersoner?** • Kan invitasjon til verktøyet sendes til innbyggere via Helsenorge? • Vil innbygger finne verktøyet som et av "Mine verktøy" på Helsenorge?
51	**Skal innbyggere logge inn i appen?** • Kan appen benytte innlogging via Helsenorge.no/Helsenorge-appen, slik at man får en sømløs overgang fra Helsenorge og appen?
50	**Dersom appen har følgende funksjoner, er disse funksjonene integrert med Helsenorge?** • **Selvbetjening:** Vil timeavtaler og/eller helsekontakter vises/varsles i Helsenorge? • **Dialog:** Vil innbygger kunne initiere dialog, motta og svare på meldinger/skjema/oppgaver fra Helsenorge?

Kommentert [GV17]: Forslag til endring: Fjerne dette avsnittet. Det blir ivaretatt gjennom forslag til endring ifm tabellen litt lengre ned i avsnittet.

Kommentert [GV18]: Dette er ikke plattformspesifikt for Helsenorge.

Forslag til endring:
Avsnittet bør tas ut av 4.1 og i stedet legges inn i egen seksjon i kapittel 3 hvor det i tillegg blir tilført litt mer informasjon rundt samspill, dataflyt og interoperabilitet mellom løsninger i sektoren.

Kommentert [GV19]: Forslag til endring: Erstatte med "må følgende krav oppfylles"

Kommentert [GV20]: Innholdet i tabellen er ikke i synk med det som gjelder for publisering av helseapper på Helsenorge og derfor kun delvis riktig og dekkende.

Forslag til endring:
Fjerne tabellen i sin helhet.
Veilederen bør i stedet henvise direkte til siden med forutsetninger og krav for å bli en del av verktøykatalogen (Krav: Klassifisering og godkjenning av digitale verktøy hos Norsk helsenett) fremfor at innhold må oppdateres og synkes to forskjellige steder. Siden som foreslås lenket inn er alltid oppdatert og det vil skape mindre tvil og forvirring rundt hva som er gjeldende, samtidig som arbeidet rundt oppdatering og vedlikehold over tid blir enklere både for direktoratet for e-helse og NHN.

Den konkrete lenken som bør brukes til kravene er:
https://helsenorge.atlassian.net/l/cp/LTt5ioTB
Denne er mer fast og varig og fungere bedre over tid selv om det blir gjort endringer på siden over tid.

Nr.	Spørsmål/Opplysning
	• **Innsyn:** Vil innbygger kunne få innsyn i sine data i applikasjonen via relevante tjenester i Helsenorge?
51	**Vil brukeren kunne få bistand fra foresatte eller pårørende de har gitt tilgang til på Helsenorge?** For apper med pålogging, støtter appen at pårørende kan logge på og bistå bruker?
52	**Dersom bruk innebærer behov for samtykker og senere trekking av samtykker, brukes aktuelle tjenester for å gi innbyggere helhetlig tilgang til å få oversikt over og endre på eventuelle reservasjoner og samtykker?**

til sist i kapitlet

Kommentert [GV20]: Innholdet i tabellen er ikke i synk med det som gjelder for publisering av helseapper på Helsenorge og derfor kun delvis riktig og dekkende.

Forslag til endring:
Fjerne tabellen i sin helhet.
Veilederen bør i stedet henvise direkte til siden med forutsetninger og krav for å bli en del av verktøykatalogen (Krav: Klassifisering og godkjenning av digitale verktøy hos Norsk helsenett) fremfor at innhold må oppdateres og synkes to forskjellige steder. Siden som foreslås lenket inn er alltid oppdatert og det vil skape mindre tvil og forvirring rundt hva som er gjeldende, samtidig som arbeidet rundt oppdatering og vedlikehold over tid blir enklere både for direktoratet for e-helse og NHN.

Den konkrete lenken som bør brukes til kravene er:
https://helsenorge.atlassian.net/l/cp/LTt5ioTB
Denne er mer fast og varig og fungere bedre over tid selv om det blir gjort endringer på siden over tid.

Kommentert [GV21]: Forslag til endring:

Legge til følgende setning til sist i avsnittet:
"Har man gjennomgått anbefalte krav for kvalitetssikring av helseapper og digitale verktøy eller blitt CE-merket, vil dette bli gjenbrukt i prosess for å tilgjengeliggjøres på Helsenorge."
h