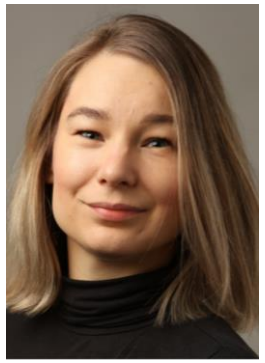
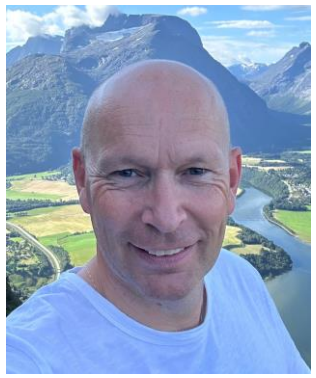
Samling for sikkerhetsledere, -rådgivere og -koordinatorer

20. november 2023



Thea Rølsåsen

Andrea Dahl Spone (NHN)



André Meldal (NHN)

Aasta Hetland (sekretariatsleder)

Jan Gunnar Broch (avdelingsdirektør)

John Marius Solli

Knut Herje

Susanne Helland Flatøy

Inger Anne Tøndel

Geir-Erlend Myhre Johansen

Marie Strand Schildmann

Tonje Stegavik

Sekretariatet for Normen

Velkommen til samling

- Sekretariatet for Normen har arrangert flere samlinger for PVO, og arrangerer i dag den andre samlingen for Sikkerhetsledere

- Disse arenaen for kunnskap- og erfaringsdeling er noe vi ser det er behov for i sektoren
  - Samlingen for PVO i April 23 var fulltegnet
  - Det er en økning i antall påmeldte til Sikkerhetsleder.

Samlinger – sosial kontrakt

- Samlingen skal være en trygg arena
- Trygt å dele, trygt å være uenige
- Hvem som har sagt hva forblir igjen på samlingen
  - Ta med deg erfaringen til andre, men ikke hvor de kommer fra.
- Vær en aktiv deltager
- Bilder er frivillig – si ifra til en av oss i sekretariatet hvis du ikke ønsker å bli med på bilder

Agenda

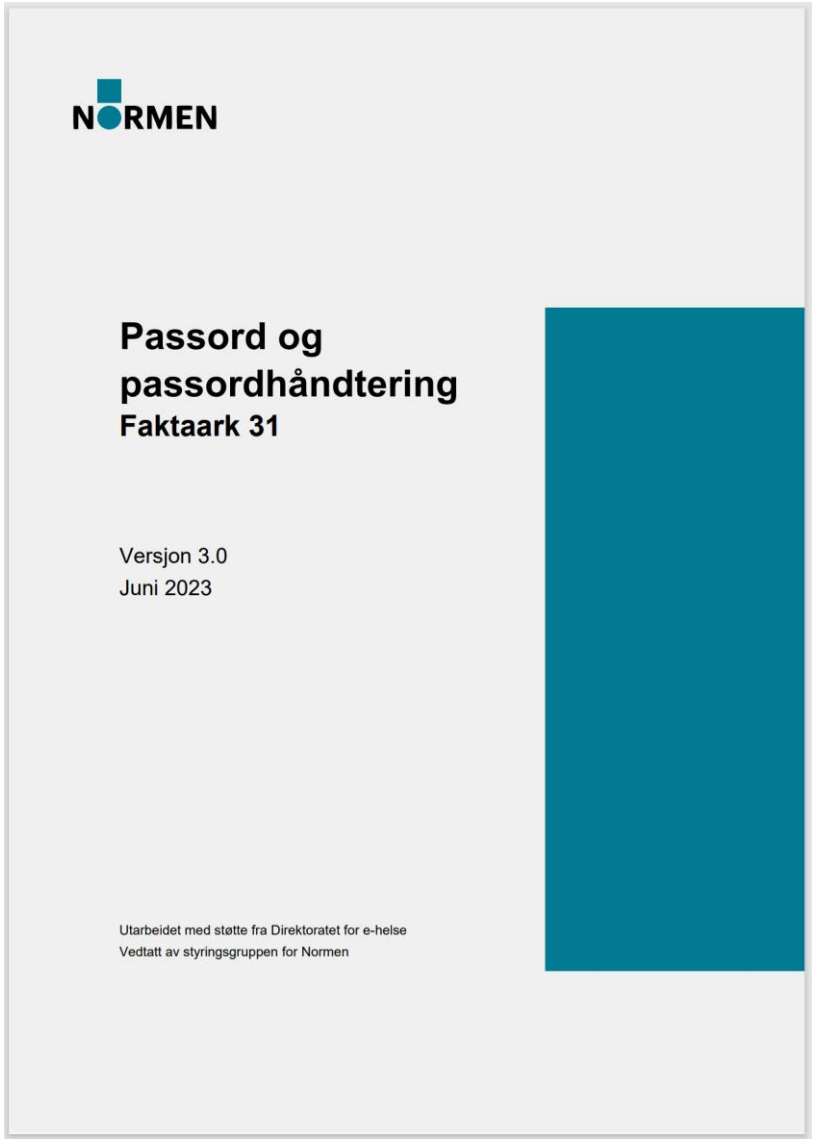
- Faktaark om passord og passordhåndtering (Knut)
- Retningslinje om bruk av helse- og personopplysninger til test og utvikling (GE)
- Leverandørveilederen (GE)
- Veileder i bruk av skytjenester til behandling av helse- og personopplysning(JMS)
- Bruk av Normens krav i anskaffelser (GE)
- Pågående aktiviteter; Kvalitet, int; Små virksomheter; JMS

Faktaark om passord og passordhåndtering

- Passord – fortsatt (nesten) like aktuelt!
- Ny utgave i juni av faktaarket

- Formål: gi veiledning i hvordan virksomheten kan sikre at passord som benyttes i virksomheten er underlagt tilstrekkelig sikring

- Faktaarket har en praktisk tilnærming og inneholder beste praksis knyttet til passord og passordhåndtering



Gi meg eksempel på et nokså dårlig passord.

Genererer svar for deg ...

Dine personlige data og firmadata er beskyttet i denne chatten

Et eksempel på et nokså dårlig passord er **123456789**. Dette passordet bryter med flere av rådene fra nettvett.no og NDLA om hvordan man lager sterke passord:

- Det er kort, bare 9 tegn.
- Det er ikke unikt og lett å gjette.
- Det inneholder bare tall og ingen symboler, store/små bokstaver eller mellomrom.
- Det er et ord som finnes i en ordliste og er ofte brukt som et standard passord.
- Det er knyttet til tjenesten passordet gjelder for, for eksempel et telefonnummer.

Dette passordet er nokså dårlig fordi det er svært utsatt for brute-force angrep, der hackere prøver å knekke passordet ved å prøve alle mulige kombinasjoner av tegn. Det er også et av de mest brukte passordene i verden, noe som gjør det enda mer sårbart. Ifølge en rapport fra NordPass, var **123456789** det nest mest populære passordet i 2020, med over 7 millioner brukere. Det tok bare mindre enn et sekund å knekke det. Du bør derfor unngå å bruke slike passord og heller følge rådene for å lage sterke passord.

Gi meg et eksempel på et godt passord.

Søker etter: **hvordan lage et godt passord**

Genererer svar for deg ...

Dine personlige data og firmadata er beskyttet i denne chatten

Et eksempel på et godt passord er **Hesten min heter 42!**. Dette passordet følger noen av rådene fra nettvett.no [1] og NDLA [2] om hvordan man lager sterke passord:

- Det er langt, minst 5 ord eller 16 tegn.
- Det er unikt og bare du husker det.
- Det inneholder både tall, symboler, store/små bokstaver og mellomrom.
- Det er ikke et ord som finnes i en ordliste eller navnet på en person, et tegn, et produkt eller en organisasjon.
- Det er ikke knyttet til tjenesten passordet gjelder for.

Gi meg et eksempel på et veldig trygt passord.

Genererer svar for deg ...

Dine personlige data og firmadata er beskyttet i denne chatten

Et eksempel på et veldig trygt passord er **!@#%&*()_+QwErTyUiOp{}|:<>?**. Dette passordet følger noen av rådene fra nettvett.no og NDLA om hvordan man lager sterke passord, men det er enda mer komplekst og tilfeldig:

- Det er langt, 20 tegn.
- Det er unikt og vanskelig å gjette.
- Det inneholder bare symboler, store/små bokstaver og ingen mellomrom.
- Det er ikke et ord som finnes i en ordliste eller navnet på en person, et tegn, et produkt eller en organisasjon.
- Det er ikke knyttet til tjenesten passordet gjelder for.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Innhold i faktaarket om passord og passordhåndtering

- Relevante bestemmelser, standarder, rammeverk
- Avgrensning
- Hva sier Normen om passord
- Trusler mot passord
- Prosedyrer for passord og passordhåndtering
- Hensyn ved utforming av passordpolicy
- Krav til bruk av passord
- Gode råd for passordhåndtering
- Eksempel på gode passord
- Håndtering av passord i systemene
- Autentisering uten bruk av passord
- Avvik til anbefalingene
- Annet veiledningsmateriell

Veien videre …

- **Webinar** om passord og passordhåndtering før jul, med ekspert-gjester
- Vi ønsker deres innspill og erfaringer om passord og passordhåndtering!

  Ta gjerne en prat med oss eller send til sikkerhetsnormen@ehelse.no

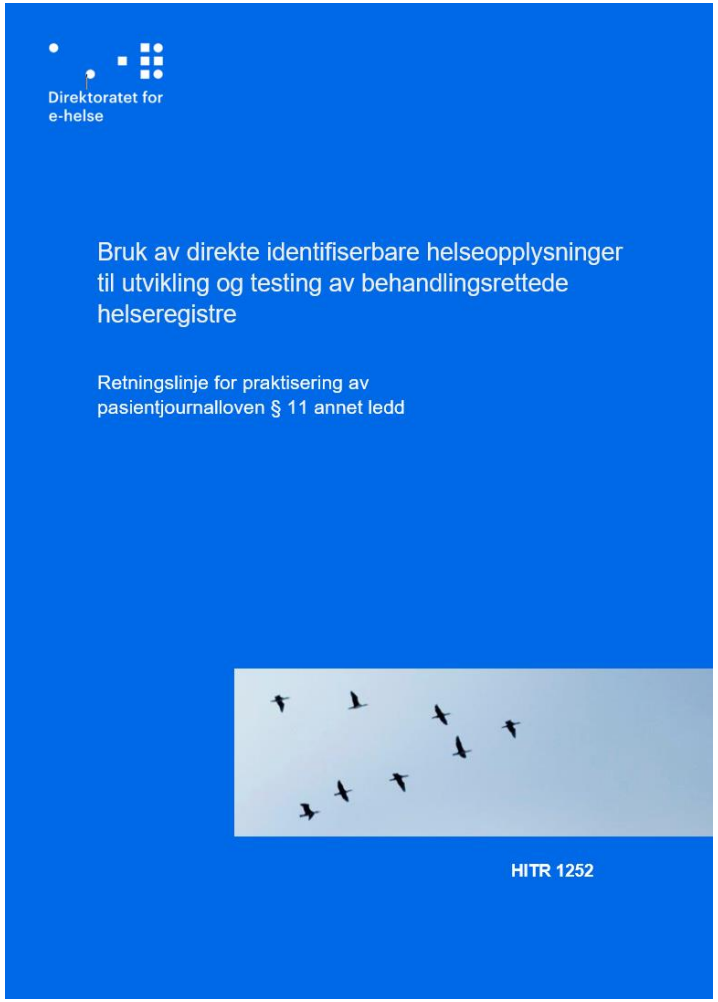
Retningslinje om bruk av helse- og personopplysninger til test og utvikling (GE)

Bakgrunn

Stortinget vedtok 10. juni 2022 et nytt annet ledd i pasientjournalloven § 11, angående bruk av helseopplysninger til utvikling og testing av behandlingsrettede helseregistre. Bestemmelsen har følgende ordlyd:

«Direkte identifiserbare helseopplysninger kan behandles i lukkede testmiljøer for å utvikle og teste behandlingsrettede helseregistre dersom det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke pseudonyme, anonyme eller fiktive opplysninger».

Det presiseres i pasientjournalloven § 11 fjerde ledd at helseopplysningene i disse tilfellene kan behandles uten hinder av taushetsplikt, og at det ikke er nødvendig å innhente samtykke fra pasienten.



Målgruppe

Retningslinjen er relevant for virksomheter skal planlegge, beslutte eller gjennomføre utvikling eller testing av behandlingsrettede helseregistre med helseopplysninger.

Retningslinjen retter seg mot alle personer som blir involvert i prosessen, både ledere, helsepersonell, øvrige ansatte og innleid personell.

Retningslinjen er særlig relevant for personell innen **fagområdene informasjonssikkerhet**, personvern, IT og medisinsk teknologi.

Dersom den dataansvarlige beslutter å engasjere en leverandør til å utføre utviklings- og testoppgaver, vil retningslinjen gjelde tilsvarende for leverandøren og eventuelle underleverandører.

Dette omfatter også IKT-driftsorganisasjoner i spesialisthelsetjenesten og virksomheter i interkommunale samarbeid. Den dataansvarlige bør instruere leverandører om å følge retningslinjen, og vurdere om det er behov for tilføyelser til databehandleravtalen.

Dersom to eller flere virksomheter har delt dataansvar for det behandlingsrettede helseregisteret, må det være avklart mellom partene hvilken virksomhet som skal ha ansvaret for utviklingen eller testingen.

Behovet…

- Retningslinjen vil av mange oppfattes som en innskjerping
- Mange i sektoren er ukjent hvilke krav som gjelder når helse- og personopplysninger benyttes til test og utvikling.
- I mange tilfeller er det lettere å benytte reelle opplysninger, enn å fremskaffe syntetiske data.

Vilkår for å bruke helseopplysninger til utviklings- og testformål

- Utviklingen må skje i et lukket testmiljø
- Formålet må være å utvikle og teste behandlingsrettede helseregistre
- Kan formålet oppnås ved å benytte fiktive, anonyme eller pseudonyme opplysninger?

- Vurderingen av vilkåret «umulig eller uforholdsmessig vanskelig»
- Pasientsikkerhet
- Oppfyllelse av pasientrettigheter
- Tid og ressursbruk
- Ekstraordinære hendelser

Forutsetninger

Tiltak for å lukke et utviklings- og testmiljø

- Separate utviklings- og testmiljøer
- Kompetanse og taushetsplikt
- Dataflyt
- Testplan
- Vurdere datagrunnlaget
- Tilgangsstyring og kontrollrutiner
- Logging
- Sletting

Øvrige forhold virksomheten må vurdere

- Rettslig grunnlag for behandling av helseopplysninger til utvikling og testformål
- Databehandleravtale
- Oppdatering av behandlingsprotokollen
- Innebygd personvern
- Dataminimering

Veileder for Informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren

- Godkjent av Styringsgruppen for Normen 08.06.23
- Veilederen beskriver tiltak og forventninger til IKT-løsninger, medisinsk utstyr og operasjonell teknologi (OT) fra leverandørens perspektiv.
  - To vedlegg
    - HUKI-Matrise
    - Flytskjema som viser innføringsprosess
- Referansegruppe bestående av:
  - IT-leverandør til sektoren
  - Flere leverandører av Medisinsk utstyr
  - Driftsorganisasjoner innen spesialist (IT og med-tek)
  - Sykehusinnkjøp og Norsk helsenett
  - Innkjøpskompetanse i kommune

Bruk av Normens krav i anskaffelser (GE)

Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren Versjon 6.1					
Krav.nr	Overordnede kapittel i Normen	Kap. i Normen	Kravbeskrivelse	Tekst for bruk i kravspesifikasjon - Leverandøren er databehandler	T I (
077.	C. Grunnleggende om behandling av helse- og personopplysninger	4.2.3 Innsyn (Plikter og krav ved behandling av helse- og personopplysninger)	Virksomheten skal sikre at den registrerte kan få innsyn i egen logg over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.	Tilbuder skal sikre at pasieter og brukere som blir registert i systemet kan få innsyn i hvem og virksomhetsilknytning til den som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt. Det bør legges til rette for at oppdragsiver skal kunne adminsiterer og hente ut innsynslogger uten å måtte involvere tilbyder.	

Kravbeskrivelse	Tekst for bruk i kravspesifikasjon - Leverandøren er databehandler
Virksomheten skal sikre at den registrerte kan få innsyn i egen logg over hvem, og fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt.	Tilbuder skal sikre at pasieter og brukere som blir registert i systemet kan få innsyn i hvem og virksomhetsilknytning til den som har tilegnet seg hvilke opplysninger, og på hvilket tidspunkt. Det bør legges til rette for at oppdragsiver skal kunne adminsiterer og hente ut innsynslogger uten å måtte involvere tilbyder.

Oppdatert Veileder i bruk av skytjenester til behandling av helse- og personopplysninger

- Mindre oppdatering av Normens skyveileder.

- Noe tilleggstekst om blant annet Zero Trust, bruk av Normen krav i anskaffelser og kontrollspørsmål til leverandører, og overføring av personopplysninger utenfor EU/EØS

Noen av de pågående aktiviteter

- Forslag til Lov om digital sikkerhet (Normen og NSM gr.pr.ikt-sikkerhet)
  - Loven skal **forplikte virksomheter** som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å **overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser.**
- Revisjon Faktaark 20a,b,c – Sikkerhet- og samhandlingsarkitektur
- KI
  - Det nasjonale koordineringsprosjektet for KI
  - Tverretatlig veiledningstjeneste for KI i helse
- Revidering veileder små virksomheter
- Faktaark integritet- «Hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen»
- Webinar
  - Digitalt introkurs Normen 14.12
  - Ny adekvansbeslutning USA
  - NIS2

NIS2

- Tydeligere krav til hele sikkerhetsområdet enn NIS1
- NIS2 dekker helsesektoren bredere enn NIS1
- NIS-2 er vurdert som EØS-relevant av Justisdepartementet, og det jobbes med å få direktivet inn i norsk lov
- Cyber Solidarity Act styrker felles evne til deteksjon, situasjonsforståelse og respons
- Cyber Resilient Act kobler seg til sektorens helselovgivning: medisinsk utstyr, EHDS

- NIS2 krav som helt, eller delvis, ikke er dekket i Normen
  - Incident handling – omforent varsling, rapportering, klassifisering, etterforskning, kommunikasjon
  - Virksomhetskontinuitet- backup management, disaster recover, crisis management
  - Sikkerhet i forsyningskjeden (verdikjeden)
  - Sikkerhet ved anskaffelse, utvikling og vedlikehold av nettverk og informasjonssystemer, inkludert håndtering av sårbarheter og deteksjon
  - Retningslinjer og prosedyrer for å vurdere effekten av tiltak for risikostyring innenfor cybersikkerhet.

Kilde: https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/