Direktoratet for e-helse

NUFA

4. – 5. september 2019

Thon Hotel Arena, Lillestrøm

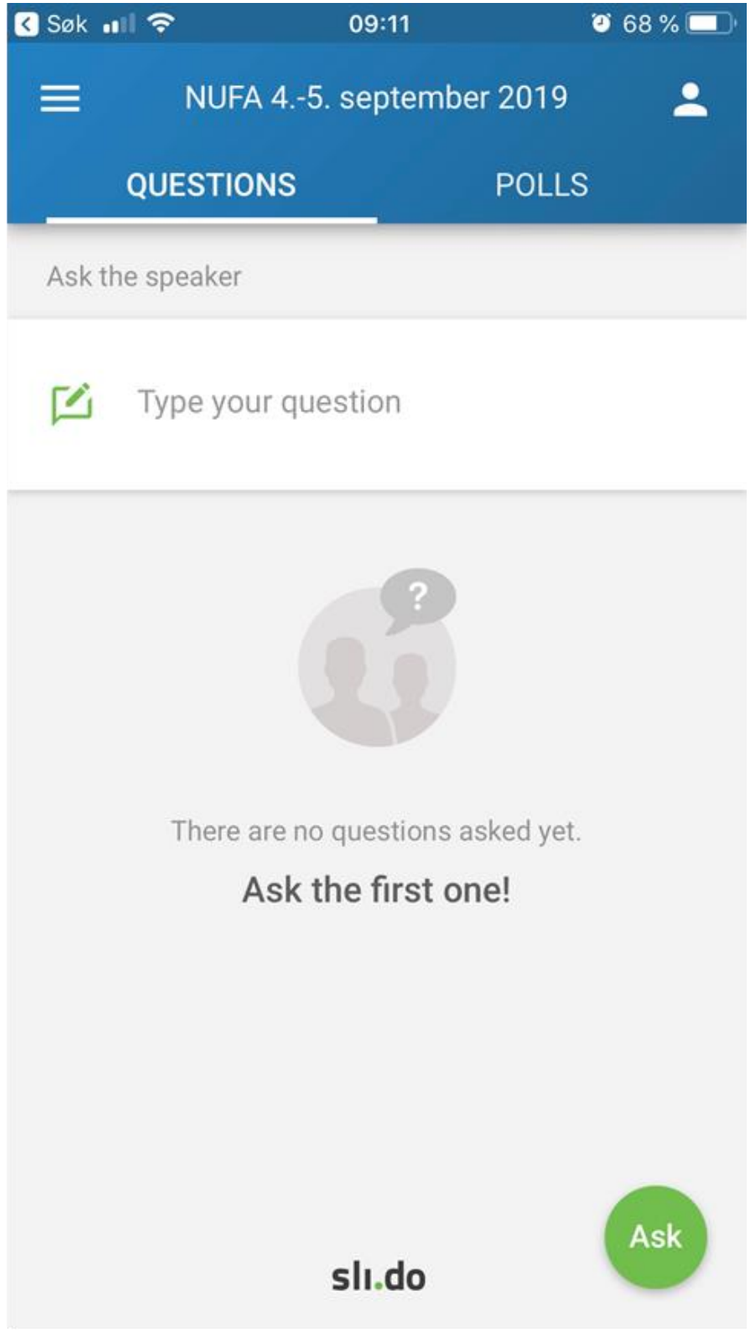
Saker 5. september –
Tema: Personvern, informasjonssikkerhet og beredskap

	Torsdag 5. september 2019						
	TEMA: Personvern, informasjonssikkerhet og beredskap						
Saksnr.	**Tittel**	**Sakstype**	**Sakseier**	**Holder presentasjonen**	**Start**	**Varighet**	**Slutt**
	Velkommen		Inga Nordberg		08:30	00:05	08:35
33/19	**Introduksjons til tema**				08:35	00:15	08:50
	Introduksjon og inspirasjon	Orientering					
	• Cybersikkerhet i min egen personlige kritiske infrastruktur			Marie Moe, Sintef	08:50	00:40	09:30
	• Hvordan kan personvern og informasjonssikkerhet bygges inn i e-helseløsninger?			Jenny Marie Ellingsæter, Sopra Steria	09:30	00:30	10:00
	Pause				10:00	00:15	10:15
	• HelseCERT			Gunnar Johansen, NHN	10:15	00:30	10:45
	• ROS IKT			Jan Gunnar Broch	10:45	00:15	11:00
34/19	**Normen**	Drøfting		Aasta Hetland	11:00	00:15	11:15
	Intro til arbeid i stasjoner				11:15	00:15	11:30
	Lunsj				11:30	00:45	12:15
	Stasjoner				12:15	01:30	13:45
	Oppsummering				13:45	00:10	13:55
35/19	**Eventuelt**				13:55	00:05	14:00
	Slutt dag 2				**14:00**		

SLIDO

- Gå inn på **slido.com**
- Tast inn eventkode: **#C479**

- Skriv inn navnet ditt i høyre hjørne
- Tast inn evt. spørsmål du må ha i løpet av presentasjonene ☺



Direktoratet for e-helse

Questback – evaluering

Sendes ut i løpet av dagen

Direktoratet for e-helse

Sak 33/19:
Tema: Personvern, informasjonssikkerhet og beredskap

NUFA 4. - 5. september 2019

TEMA

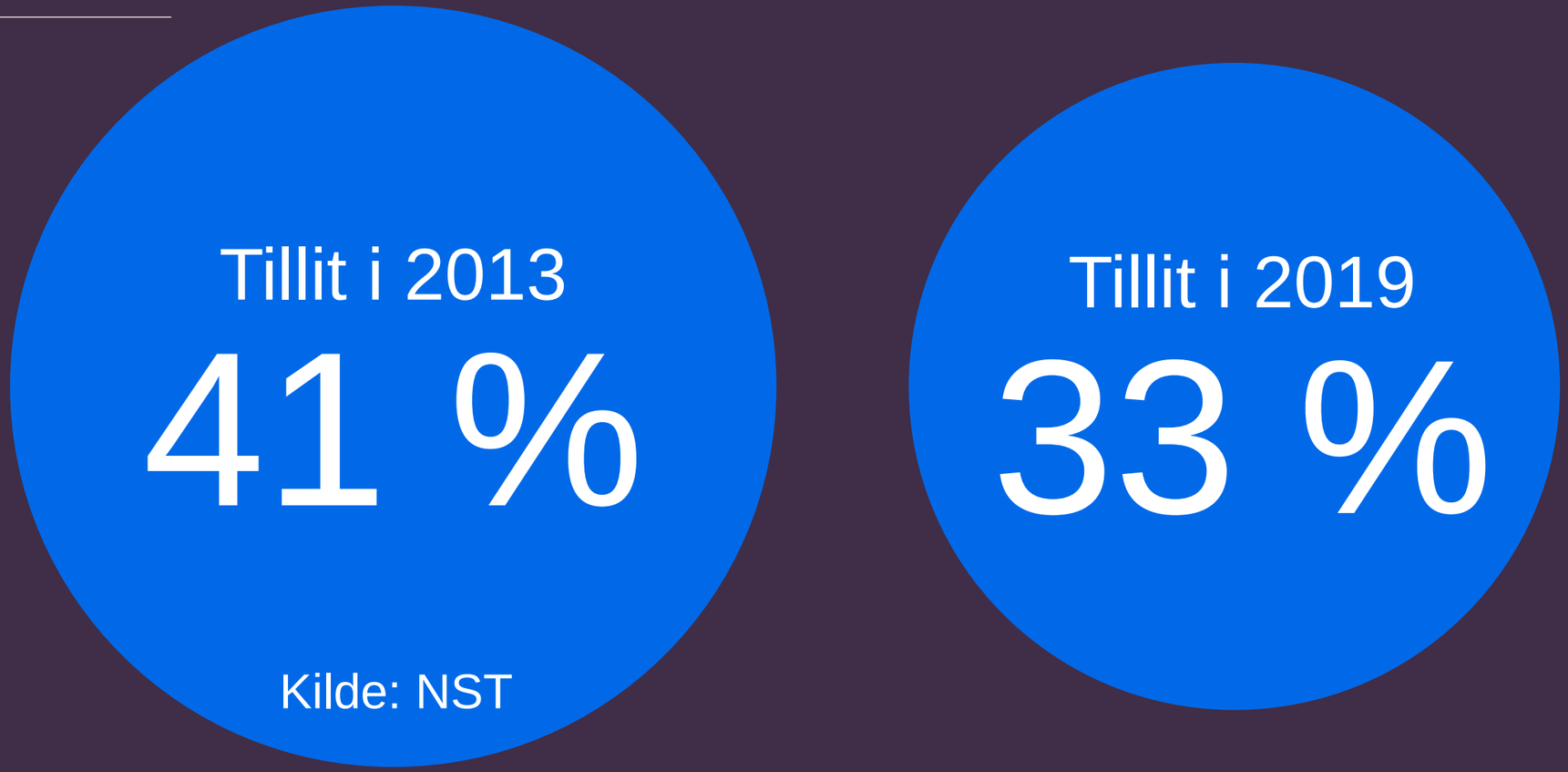
- Beredskap
- Informasjonssikkerhet
- Personvern

Strategisk plan for e-helse består av 14 innsatsområder underlagt strategiens seks strategiske satsingsområder

Digitalisering av arbeidsprosesser	Bedre sammenheng i pasientforløp	Bedre bruk av helsedata	Helsehjelp på nye måter	Felles grunnmur for digitale tjenester	Nasjonal styring av e-helse og økt gjennomføringsevne
1.1 Modernisere journalløsninger	2.1 Bidra til plan og kontinuitet i ansvarsoverganger	3.1 Bedre behandling med bedre utnyttelse av helsedata	4.1 Tilrettelegge for innbyggeren som ressurs	5.1 Utvikle felles byggeklosser som tilrettelegger for enhetlig samhandling	6.1 Skape en nasjonal leveransekraft
1.2 Digitalisere legemiddelkjeden innenfor hver virksomhet	2.2 Dele oppdatert legemiddelopplysninger	3.2 Bedre bruk av helsedata til sekundærformål	4.2 Stimulere til innovasjon	5.2 Helhetlig og effektiv styring og forvaltning av byggeklossene i felles grunnmur	6.2 Styrke arbeidet med innføring og sikre at gevinster oppnås
			4.3 Helsehjelp og omsorg på avstand		**6.3 Styrke arbeidet med beredskap, informasjonssikkerhet og personvern**

Respondentenes tillit til at helseopplysningene deres er tilgjengelige i en akutt situasjon faller

Innbyggerundersøkelsen 2019



Tall fra 2013: NST; Prosjektrapport e-helse i Norge 2013, https://ehealthresearch.no/prosjektrapporter/arkiv/e-helse-i-norge-2013

Kun 55 % har tillit til at helseopplysningene deres er lagret slik at utenforstående ikke har tilgang til dem

Innbyggerundersøkelsen 2019

AGENDA

- **Cybersikkerhet i min egen personlige kritiske infrastruktur**
  - Marie Moe, Sintef
- **En praktisk tilnærming til innebygd personvern**
  - Jenny Marie Ellingsæter, Sopra Steria
- **HelseCERT – trusler og sårbarheter**
  - Gunnar Johansen, Norsk Helsenett
- **Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren**
  - Jan Gunnar Broch, Direktoratet for e-helse
- **Normen 6.0**
  - Aasta M. Hetland, Direktoratet for e-helse
- **Stasjoner:**
  - Innebygd personvern, Normen 6.0, Cybersikkerhet og beredskap

Direktoratet for e-helse

Sak 33/19:
Cybersikkerhet i min egen personlige kritiske infrastruktur

Marie Moe

NUFA 4. - 5. september 2019

Direktoratet for e-helse

Sak 33/19:
Hvordan kan personvern og informasjonssikkerhet bygges inn i e-helseløsninger?

Jenny Marie Ellingsæter

NUFA 4. - 5. september 2019

Innebygd personvern i praksis

Jenny Marie Ellingsæter

05.09.2019

sopra steria

Lost in translation

“Personvern” vs. “Data protection”

Innebygd

Proaktiv istedenfor reaktiv, og som **del av løsningsdesignet fra start**.

Som standardinnstilling

Den mest **personvernfremmende** innstilling på som **standard**.

Eksempel – Innebygd personvern

tps://toyen.osloskolen.no/for-elever-og-foresatte/hjemskole-samarbeid/skolemelding/

Slik melder du fravær for ditt barn via appen:

1 Klikk på "Ny melding", og knappen "Meld fravær".

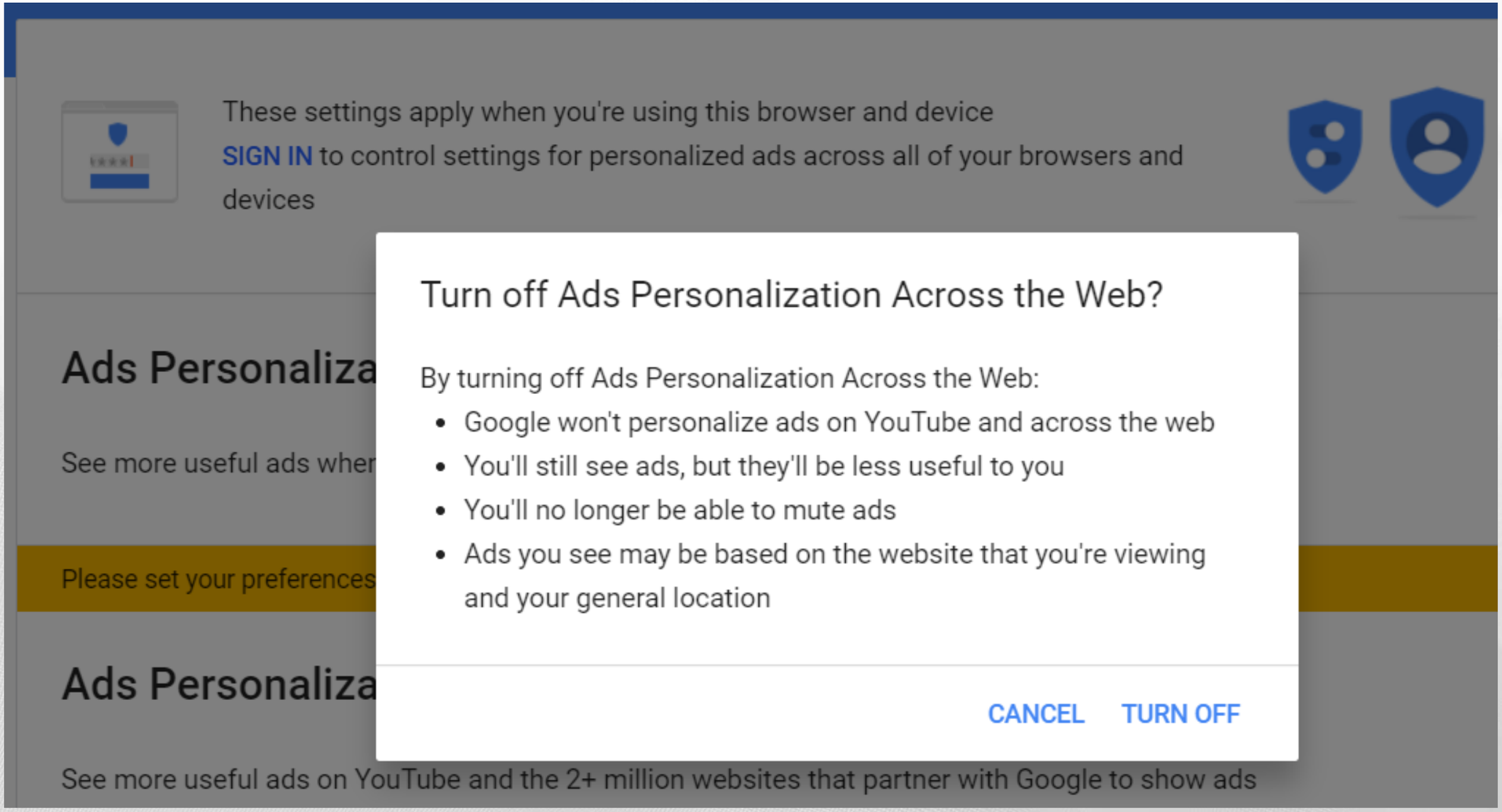
2 Velg hvilket av barna du skal melde fravær for. Hvis barnet er tilknyttet flere skoler, velger du hvilken skolen det gjelder.

3 Velg tidspunkt for fravær (i dag, i morgen eller dato) og eventuelt klokkeslett

4 Trykk Send.

På grunn av personvernhensyn kan du ikke skrive noe om grunnen til fraværet. Appen og øvrige kommunikasjonskanaler i Skoleplattform Oslo skal ikke brukes til å sende sensitive personopplysninger, som ditt barns helseopplysninger. Det holder å si at barnet ikke kommer på skolen i dag.

Eksempel – Som standardinnstilling



Hva er det som skal «bygges inn»?

*«integrere de nødvendige garantier i behandlingen for å **oppfylle kravene i denne forordning** og verne de registrertes rettigheter.»*


Innebygd personvern og personvern som standardinnstilling
Rett til å protestere
Profilering
Data-minimering
Lovlighet
Samtykke
Formåls-begrensning
Riktighet
Rett til innsyn
Ansvar
Risiko for de registrerte
Integritet
Rett til dataportabilitet
Sikkerhet ved behandlingen
Rett til sletting
Konfidensialitet
Åpenhet
Lagrings-begrensning
Rett til begrensning
Rettferdighet
Rett til retting
Hendelses-håndtering
Tilgjengelighet
Automatiserte avgjørelser

Viktige områder å ta hensyn til

Grunnleggende prinsipper

- Lovlighet, rettferdighet og åpenhet
- Formålsbegrensning
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet

Den registrertes rettigheter

- Rett til innsyn
- Rett til sletting
- Rett til retting
- Rett til begrensning av behandling
- Rett til dataportabilitet

Sikkerhet ved behandlingen

Egnede tekniske og organisatoriske tiltak med hensyn til:

- Den tekniske utvikling
- Behandlingens art, omfang, formål og kontekst
- Kostnader
- Risiko for den registrerte

Avvikshåndtering

Brudd på personvernsikkerheten skal varsles uten ugrunnet opphold til tilsynsmyndigheten, og i alvorlige tilfeller også til de registrerte.

Aktuelle tiltak relatert til grunnleggende prinsipper

1. Etabler er en datamodell som støtter kravene i forordningen, slik som retting og sletting.
2. Hent personopplysninger fra pålitelige kilder, og oppdater så ofte som mulig.
3. Hold styr på formålet dataene var samlet inn for og bruk ikke opplysningene til andre formål.
4. Begrens innsamling av personopplysninger – både type informasjon og mengde.
5. Begrens mengden personopplysninger som behandles, og antall steder opplysningene behandles.
6. Hold styr på hvor personopplysninger er lagret, og når de skal slettes.

Aktuelle tiltak relatert til den registrertes rettigheter

1. Det skal være like enkelt å trekke tilbake samtykke som det er å gi sitt samtykke.
2. Hold styr på når den registrere ga sitt samtykke, og eksakt hva den registrerte samtykket til.
3. Samtykke skal innhentes for hvert separate behandlings-formål.
4. Sørge for at det er mulig å unikt identifisere den registrerte og dens personopplysninger.
5. Sørge for effektiv håndtering av innsynsbegjæringer, dataportabilitet osv.
6. Ivareta konfidensialitet og integritet hele veien fra produksjonsmiljø til den registrerte.

Aktuelle tiltak relatert til sikkerhet (del 1)

1. Etabler rutiner for kontinuerlig vurdering og verifisering av effektiviteten av sikkerhets- og personverntiltak.
2. Begrens angrepsflaten. Skru av tjenester som ikke er i bruk, skill tjenester fra hverandre og begrens tilgang.
3. Bygg sikkerhet lagvis
   - sørg for at det er flere sikkerhetsmekanismer som må feile for at et angrep eller misbruk skal lykkes.
4. Følg leverandør- og bransjestandarder for herding av systemer og tjenester.
5. Adskill personopplysninger for å bedre tilgangskontroll og begrense omfang ved hendelser.
6. Begrens tilgang basert på tjenstlig behov, og adskill arbeidsoppgaver.

Aktuelle tiltak relatert til sikkerhet (del 2)

7 Vurder å kryptere personopplysninger i ro og i bevegelse.

8 Implementer personvernfremmende tiltak slik som pseudonymisering og aggregering.

9 Autentiser datakilder og valider dataene som sendes inn til systemer.

10 Logg alle hendelser av interesse i systemet, og sikre at ingen kan benekte å ha utført en aktivitet de har utført, og vice-verse.

11 Adskill miljøer med ulike behov for sikkerhet, slik som utvikling, test og produksjon.

12 Fiks sikkerhets- og personvernsvakheter før behandling av personopplysninger tar til, og ellers så raskt som mulig.

Aktuelle tiltak relatert til avvikshåndtering

1. Sørg for at aktiviteter og hendelser i systemer og applikasjoner logges på et strukturert format.
2. Sørg for overvåkning av loggene, og etabler alarmer for uønsket eller unormal aktivitet.
3. Oppett avvikshåndteringsplaner for systemer og applikasjoner.
4. Opprett en prosess for avvikshåndtering og identifiser rollene som kreves.
5. Identifiser nøkkelpersonell og øv på avvikshendelser.
6. Før register over sikkerhetshendelser og lær.

Strategisk arbeid med sikkerhet og personvern

PROAKTIV REAKTIV

Forutse

Sikre tilstrekkelig sikkerhets- og personvern-**kompetanse**, forstå trusselbildet og egen angrepsflate, still tydelige **krav** til sikkerhet og personvern.

Forebygg

Begrens angrepsflaten, **forebygg** hendelser ved implementasjon av sikkerhets- og personverntiltak, sikre at krav er oppfylt, og **verifiser** tiltakenes effektivitet.

Detekter

Sikre evne til å så tidlig som mulig **oppdage** sikkerhetshendelser, slik som tilsiktet eller utilsiktet misbruk av tjenesten.

Responder

Sikre evne til å **håndtere** en sikkerhetshendelse rask og effektivt, begrense skaden, gjenopprette, analysere årsak og **lære**.

Takk for oppmersksomheten

Delivering Transformation. Together.

www.soprasteria.no

Direktoratet for e-helse

Pause

kl. 10:00 - 10:15

Direktoratet for e-helse

Sak 33/19: HelseCERT

Gunnar Johansen

NUFA 4. - 5. september 2019

Direktoratet for e-helse

Sak 33/19: ROS IKT

Jan Gunnar Broch

NUFA 4. - 5. september 2019

Direktoratet for e-helse

Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren

Bakgrunn

- Inngår som en av flere risiko- og sårbarhetsvurderinger som er levert Helse- og omsorgsdepartementet i 2019
  - Helsedirektoratet koordinerte arbeidet med rapportene
- Arbeidet er gjort i samarbeid med **Norsk Helsenett SF** og andre relevante aktører, i tillegg til **Helsedirektoratet**
- **Lenker til dokumentene:**
  - **helsedirektoratet.no**
  - **ehelse.no**

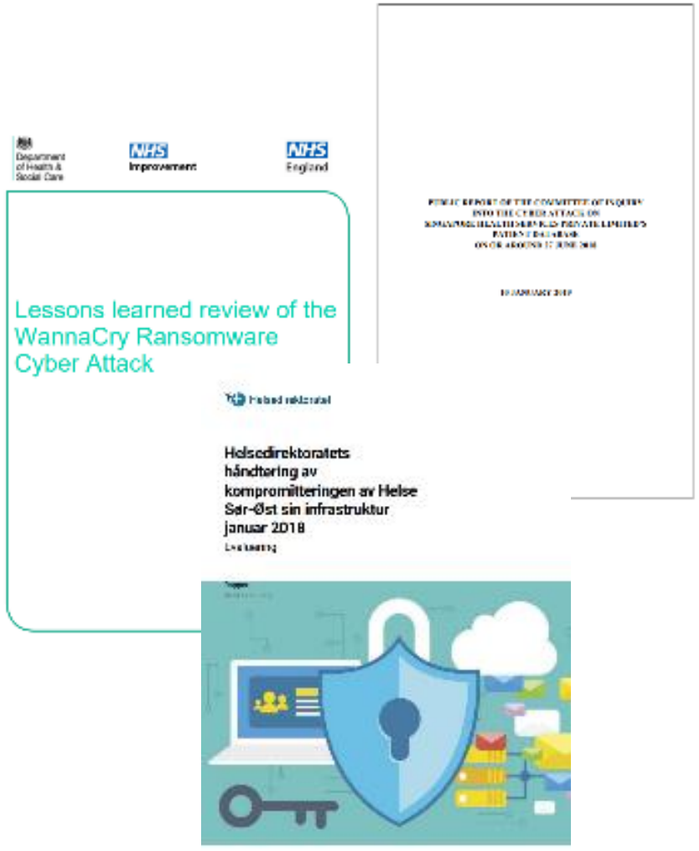
Bakgrunnsmateriale

Tar utgangspunkt i eksiterende rapporter og vurderinger:

- Utredninger

- Nasjonale trusselvurderinger

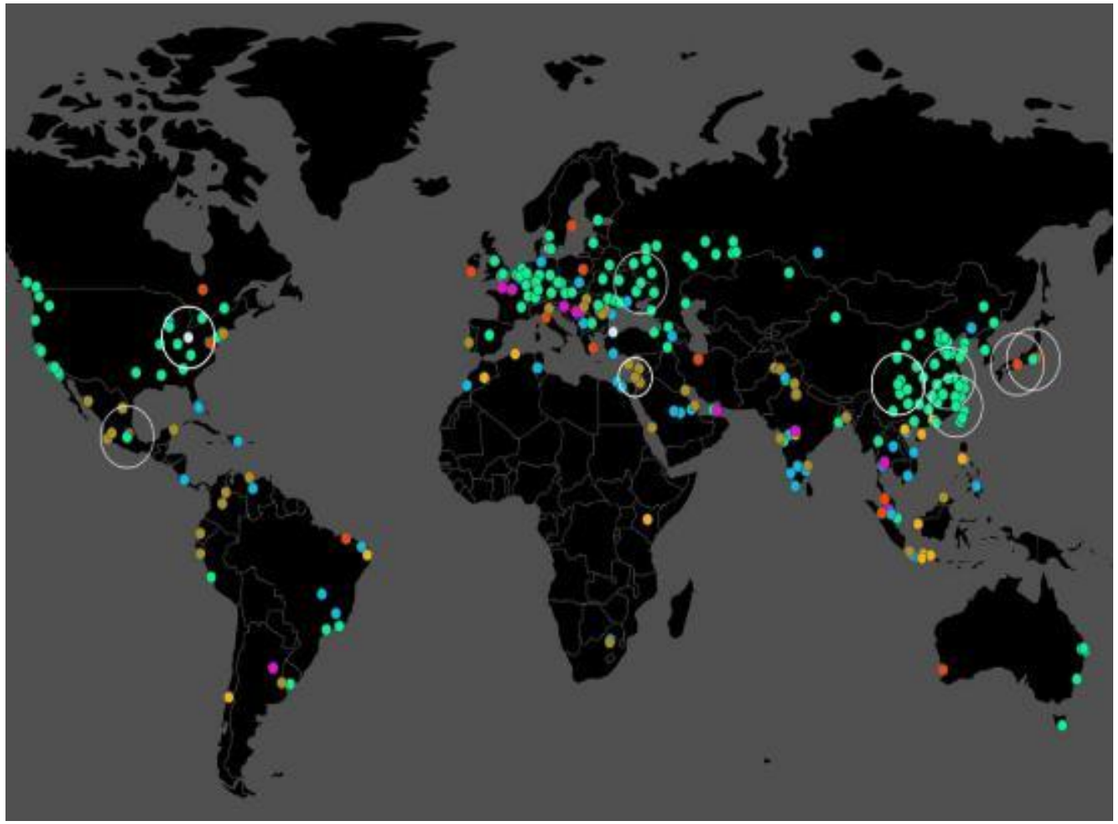
- Rapporter fra hendelser

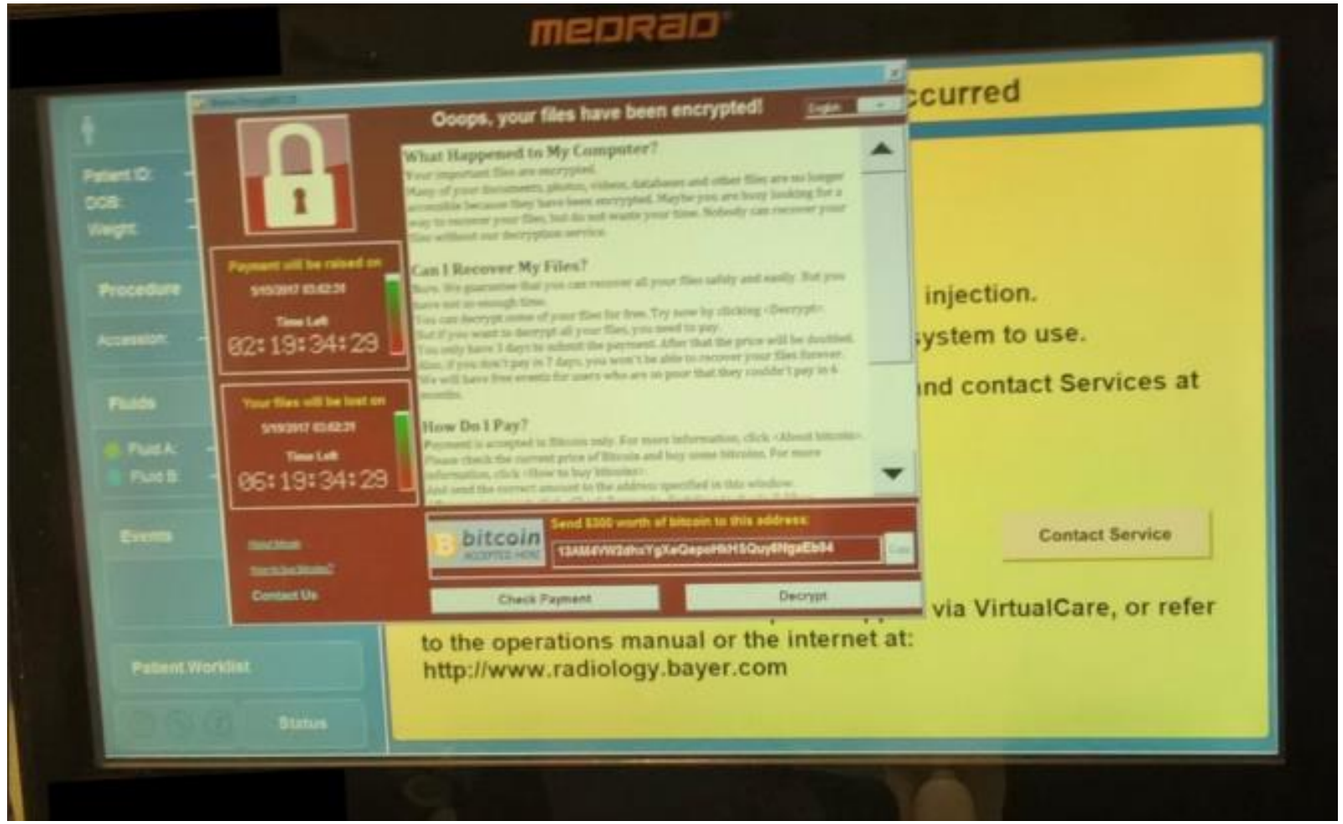


Økt digitalisering, flere sammenkoblede systemer og mer utveksling av informasjon vil skape **bedre tjenester for pasientene** og nye gevinster for sektoren, men i**ntroduserer samtidig nye trusler og sårbarheter**

Trusselbilde og eksempler på hendelser

Mai 2017:Ransomware mot NHS





Estimert kostnad > 1 milliard kroner

https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#6a7fb780425c

Januar 2018: Dataangrep mot Helse Sør-Øst

Aftenposten A-magasinet Osloby Sport Meninger Jan Gunnar Meny

Pasientinformasjon kan være på avveie etter dataangrepet mot Helse sørøst

Myndighetene utelukker ikke at pasientinformasjon er på avveie i det som betegnes som et organisert, komplekst og sammensatt dataangrep mot Helse sørøst.

FOTO: Larsen, Håkon Mosvold / NTB scanpix

Helseminister Bent Høie og justis-, beredskaps- og innvandringsminister Sylvi Listhaug holder pressebrief i forbindelse med dataangrepet mot Helse Sør-Øst.

Bergens Tidende BT Magasinet Sport Kultur Meninger Bli abonnent Meny

Innenriks

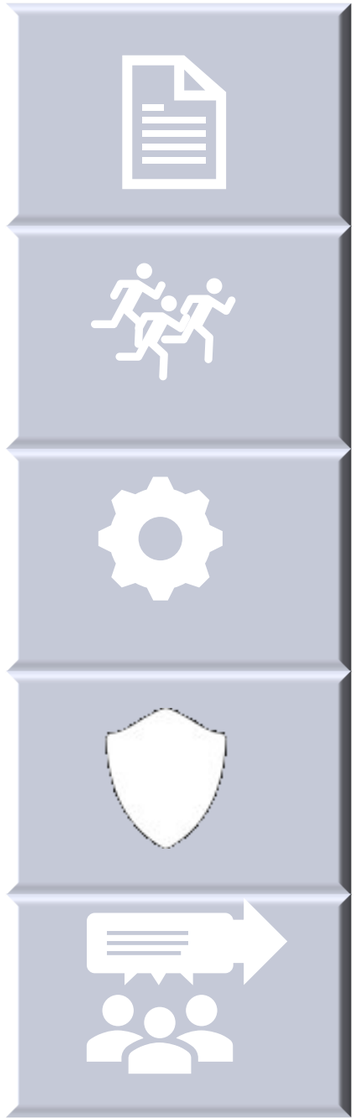
POLITIET: Påtaleansvarlig Line Nyvoll Nygaard fra PST under pressekonferansen om nettverksangrep mot datasystemene til Helse sør-øst. FOTO: NTB SCANPIX

PST etterforsker dataangrepet mot Helse sørøst som mulig etterretningsvirksomhet

Økt **digitalisering**, flere **sammenkoblede** systemer og mer **utveksling** av informasjon vil skape **bedre tjenester** for pasientene og nye gevinster for sektoren, men **introduserer samtidig nye trusler og sårbarheter:**

- Lange, komplekse og uoversiktlige **verdikjeder**
- Manglende **IKT-sikkerhetskompetanse**
- Mangelfull **implementering** av tekniske sikkerhetstiltak
- **Utdatert** programvare og utstyr som ikke oppdateres
- Mangel på og mangelfull etterlevelse av **styringssystem** for informasjonssikkerhet
- Manglende **planverk og trening** i håndtering av IKT-hendelser

Foreslåtte tiltak



Tiltak

1	Utarbeidelse av **nasjonal IKT-beredskapsplan** for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan
2	Gjennomføre årlig **IKT-øvelse**
3	**Styrket operativ** IKT-sikkerhet i helse og omsorgssektoren
4	**Styrket myndighetsrolle** for IKT-sikkerhet i helse- og omsorgssektoren
5	Utarbeidelse av **helhetlig IKT-sikkerhetsstrategi** for helse- og omsorgssektoren

I tråd med plan for gjennomføring av oppdraget, har tiltakene nasjonalt fokus og myndigheter og nasjonale aktører som tiltakseiere

1

Utarbeidelse av **nasjonal IKT-beredskapsplan** for helse- og omsorgssektoren som en del av Nasjonal helseberedskapsplan

- Planen bør bl.a. omfatte tiltak for å hindre spredning eller avverge ytterligere angrep mot IKT-infrastruktur under en hendelse.

- ***Ansvarlig****: Helse- og omsorgsdepartementet som ansvarlig for Nasjonal helseberedskapsplan*
- ***Frist****: Utkast bør være klart til å testes i den nasjonale øvelsen Digital 2020*

2 Gjennomføre årlig **IKT-øvelse**

- Det bør årlig gjennomføres en øvelse på **IKT-scenarier** som får konsekvenser for helsesektoren.
- Øvelsen bør sees i sammenheng med Nasjonal helseøvelse.

- ***Ansvarlig**: Helsedirektoratet*
- ***Frist**: Årlig fra 2020*

3 **Styrket operativ IKT-sikkerhet** i helse og omsorgssektoren

- HelseCERT bør
  - gi ut **årlige anbefalinger** om basistiltak for økt operativ IKT-sikkerhet i helsesektoren
  - **kartlegge og informere** om den generelle sikkerhetstilstanden i helse- og omsorgssektoren.
  - Tiltak som foreslås baseres på funn av sårbarheter identifisert gjennom **sårbarhetsskanning og inntrengningstesting.**

- ***Ansvarlig**: Norsk Helsenett SF*
- ***Frist**: Løpende fra 2020*

4  **Styrket myndighetsrolle** for IKT-sikkerhet i helse- og omsorgssektoren

- Direktoratet for e-helse bør styrke sin rolle som **fagorgan** for sektoren innen informasjonssikkerhet
  - **Utrede** og **foreslå** tiltak
  - Gi råd til **Statens Helsetilsyn** om «IKT-tilsyn»
  - styrke arbeidet med **opplæring og rådgivning**
  - **kartlegge og informere** om den generelle sikkerhetstilstanden i sektoren

- ***Ansvarlig****: Direktoratet for e-helse*
- ***Frist****: Løpende fra 2020*

5 Utarbeidelse av **helhetlig IKT-sikkerhetsstrategi** for helse- og omsorgssektoren

- Det bør utarbeides en **helhetlig IKT-sikkerhetsstrategi** for helse- og omsorgssektoren.
  - IKT- sikkerhetsstrategien bør ses opp mot nasjonal strategi for IKT-sikkerhet
  - ta høyde for sektorspesifikke utfordringer og utvikling av dagens helsetjeneste.

- ***Ansvarlig**: Direktoratet for e-helse i samarbeid med sektor og kompetansemiljøer*
- ***Frist**: 2021*

NUFA tar saken til orientering og ber Direktoratet for e-helse ta med innspill fra drøftingen i videre arbeid.

Direktoratet for e-helse

Sak 34/19: Normen

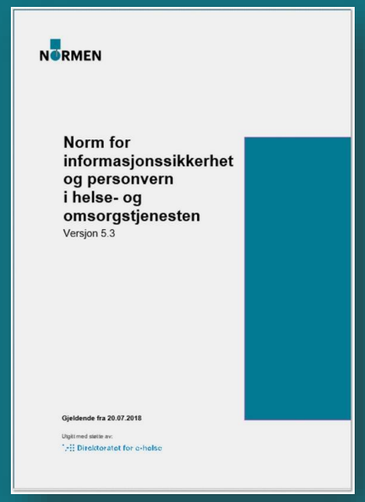
NUFA 4. - 5. september 2019

Alt om Normen på 15 minutter

- Hva er Normen?
- Litt om Normens strategi
- Ny versjon av Normen nå på høring
- Atferdsnorm etter forordningens regler

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten

Bransjenormen



Veiledning

Utadrettet virksomhet

Normkonferansen 2019

Norges første og største bransjenorm for informasjonssikkerhet – og fra 2018 også for personvern

NORMEN

Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten

Normen er til for..

.. **alle virksomheter** som ved **avtale** har forpliktet seg til å følge **Normen –** i praksis de fleste av sektorens mer enn titusen virksomheter og deres leverandører og databehandlere

Normen godkjennes og forvaltes av..

Den offentlige tannhelsetjeneste

.. en bredt sammensatt **styringsgruppe** fra sektoren

Normens daglige arbeid koordineres av..

.. et **sekretariat** plassert i Direktoratet for e-helse med fast representasjon fra Norsk Helsenett

Bakgrunn | Nåsituasjon

Sektorens utfordringsbilde | informasjonssikkerhet og personvern

- Rask teknologisk utvikling, men fortsatt mange gamle løsninger
- Trusselbilde i endring
- Store forventninger til digitalisering og samhandling
- Informasjonssikkerhet og personvern er en forutsetning for digitalisering
- Komplekst lovverk – ny personvern-forordning
- En stor del små virksomheter med begrenset kompetanse på området

Normens bevaringsområder

- **Anerkjent i sektoren, har legitimitet, og er godt etablert**
- **Sektoren står samlet bak**
- **En god arena - samarbeid og kompetanse-heving**
- **Normen som felles kravsett er nyttig for sektoren**

Normens utviklingsområder

- **Innhold oppfattes vanskelig og lite tilgjengelig**
- **Ikke dekkende på alle områder**
- **Vet lite om etterlevelse**

NORMEN STRATEGI 2019-2021

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten –sektorens felles krav, verktøy og arena for informasjonssikkerhet og personvern

Normen skal…

- bidra til at virksomheter som følger Normen har egnede tekniske og organisatoriske tiltak på plass
- fremme samhandling gjennom tillit i helse- og omsorgssektoren
- fremme en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet
- forenkle arbeidet med informasjonssikkerhet og personvern

Strategi

Helse- og omsorgssektorens felles bransjenorm skal øke sin nytte og relevans gjennom

- forenkling
- tilgjengeliggjøring
- oppdatering
- effektiv utadrettet virksomhet
- tilpasning til personvernforordningen

Prioriterte temaområder

- Pasient-/brukerrettigheter og personvern
- Leverandørkrav og -oppfølging
- Sekundærbruk

Prioriterte målgrupper

- Ledelse
- Leverandører og databehandlere
- Små virksomheter

NORMEN STRATEGI 2019-2021

STRATEGISKE FOKUSOMRÅDER OG INITIATIVER

1. **Forenkling, lesbarhet og nyttige verktøy**
2. **Felles arena**
3. **Sektorens felles kravsett til informasjonssikkerhet og personvern**

Som **selvstendig næringsdrivende med en liten virksomhet** gir Normen meg

- en samlet oversikt over de krav jeg må forholde meg til
- målrettet veiledning på en et område jeg synes er vanskelig og ikke har god kompetanse på
- maler tilpasset min arbeidshverdag

Som **leverandør** gir Normen meg

- en oversikt over de minimumskrav som helsetjenesten vil stille til meg
- forutsigbarhet i hvilke krav som stilles til meg
- Et felles begrepsapparat som muliggjør samhandling

Som **leder** gir Normen meg

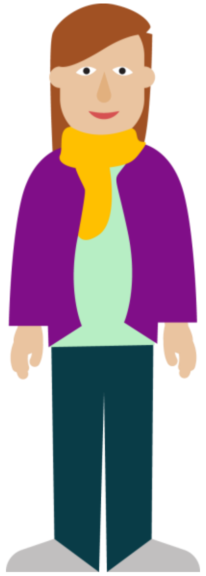
- oversikt over de minimumskrav jeg har ansvar for at min virksomhet oppfyller
- krav jeg kan stole på at også de andre lederne i sektoren vil jobbe for å oppfylle
- en arena for å diskutere prinsipielle problemstillinger på området
- Veiledning og en arena der jeg og mine medarbeidere kan få økt kompetanse
- Felles sektorkrav til bruk i anskaffelser og leverandøroppfølging
- Et felles begrepsapparat som muliggjør samhandling

Som **innbygger** gir Normen meg

- Tillit til at helsesektoren jobber for at mine opplysninger skal være trygge og tilgjengelige
- Tillit til at helsesektoren jobber for at jeg kan få oppfylt mine personvernrettigheter

For meg som jobber med informasjonssikkerhet og personvern gir Normen meg

- oversikt over de minimumskrav jeg skal bidra til at min virksomhet oppfyller
- en arena for mitt fag
- veiledningsmateriell jeg kan bruke i mitt arbeid
- Felles sektorkrav til bruk i anskaffelser og leverandøroppfølging
- Et felles begrepsapparat som muliggjør samhandling og gjennomslag for sikkerhet og personvern

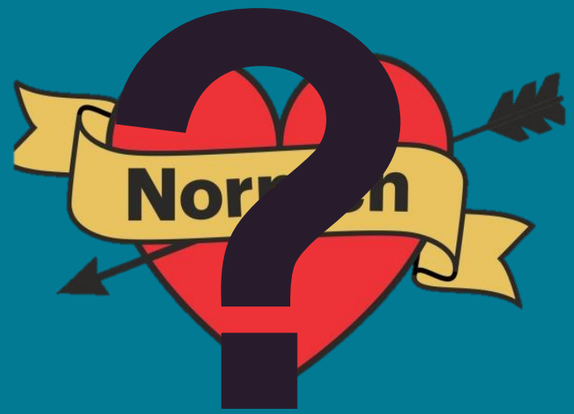


Overordnet om innholdet i versjon 6.0

- Virkeområde
- Økt leser- og brukervennligheten
  - Endrede krav, slettede krav
  - Total språklig gjennomgang
- Tydeliggjøring av hvilke krav som gjelder for hvilke virksomheter og ved hvilke behandlinger – «kan» og «bør»
- Styringssystem og risikostyring
- Sekundærbruk
- Eget kapittel om behandlingsgrunnlag og krav og plikter til virksomhetenes behandling av helse- og personopplysninger
- Kravene om leverandørforhold og avtaler er blitt klarere med tanke på hvilke krav i Normen som er relevante ut fra type leveranse og tjeneste som ytes
- Begrepet sikkerhetsarkitektur er introdusert og nye krav til informasjonssikkerhet innarbeidet
  - Kravene er harmonisert med NSMs grunnprinsipper for IKT-sikkerhet

Høringsmøte 23. september

- Åpent møte med stream
- Leverandørmøte

NORMEN + GDPR EU General Data Protection Regulation = 

Godkjenning adferdsnorm

- Normen er sendt til Datatilsynet for godkjenning
- Normen er en bransjenorm selv uten godkjenning
  - Normens krav gjelder på akkurat samme måte som den har gjort siden 2006
  - Alle nytteverdiene er de samme som før

Normkonferansen 2019

26.-27. november på The Qube – Clarion Oslo airport
Opplæringsdag 25.november

NORMEN

Direktoratet for e-helse

Lunsj

kl. 11:30 - 12:15

Tidsplan for gruppearbeid

	Gruppe 1	Gruppe 2	Gruppe 3
12:15-12:40	Innebygd personvern	Normen 6.0	Cybersikkerhet og beredskap
12:40–13:05	Cybersikkerhet og beredskap	Innebygd personvern	Normen 6.0
13:05-13:30	Normen 6.0	Cybersikkerhet og beredskap	Innebygd personvern
13:30-13:50	Oppsummering i plenum		

Innhold i gruppearbeid

1. Spørsmål / kommentarer til innlederne?

2.

Innebygd personvern	Normen 6.0	Cybersikkerhet og beredskap
Velg en nasjonal e-helse løsning som enda ikke er utviklet– hvilke tiltak kan treffes for å understøtte innebygd personvern i løsningen	Innspill til • Sikkerhetsarkitektur • Tilgangsstyring • Leservennlighet • Forholdsmessighet	Diskusjon om trusler og sårbarheter - og betydning for nasjonale e-helseløsninger Innspill til tiltakene i «Overordnet risiko- og sårbarhetsvurdering for IKT i helse- og omsorgssektoren»

NUFA ber Direktoratet for e-helse om å ta med innspill fremkommet i møtet i det videre arbeidet.

Direktoratet for e-helse

Sak 35/19: Eventuelt

NUFA 4. - 5. september 2019

Direktoratet for e-helse

Questback – evaluering

Bruk 5 min til å besvare evalueringen

Direktoratet for e-helse

Vel hjem.

Neste møte er 6. - 7. november

Scandic Lillestrøm