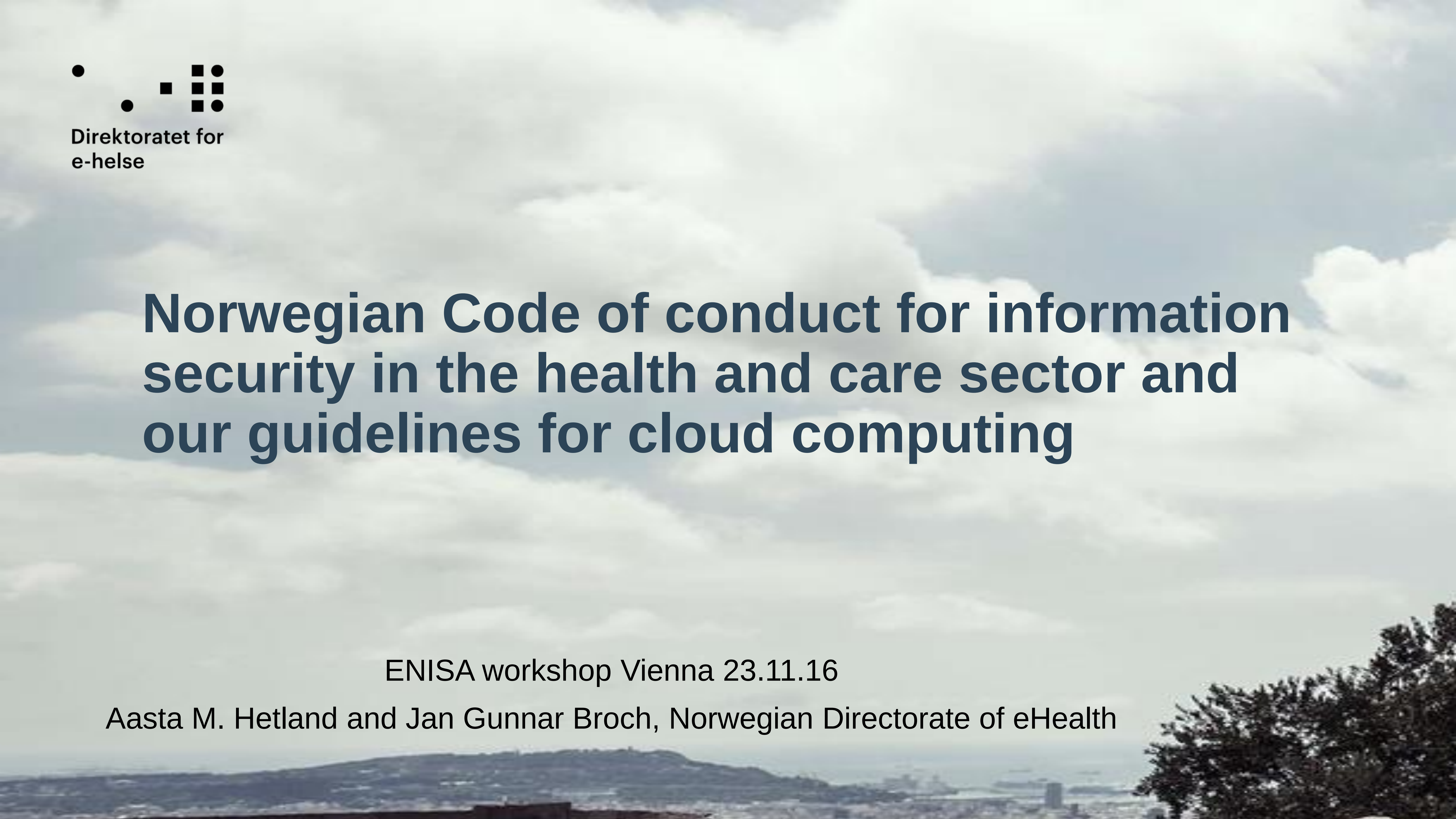


Direktoratet for
e-helse

Norwegian Code of conduct for information security in the health and care sector and our guidelines for cloud computing

ENISA workshop Vienna 23.11.16

Aasta M. Hetland and Jan Gunnar Broch, Norwegian Directorate of eHealth

Health and care services for all

Governance

Ministry of Health and Care Services
Issues laws and regulation, drafts policies and financies

Directorate of eHealth
National coordination and standardization.
Delivery of national eHealth solutions.

4 regional health authorities
Responsible for specialist health care

428 Municipalities
Responsible for primary care, GPs, public health, long term care and rehabilitation

5,2 MILLION

LIFE EXPACTANCY 81,5

4 100 GPs

GP ACTS AS GATEKEEPER

9,9% of GDP

PUBLIC FUNDING 85 %

Source: OECD 2015

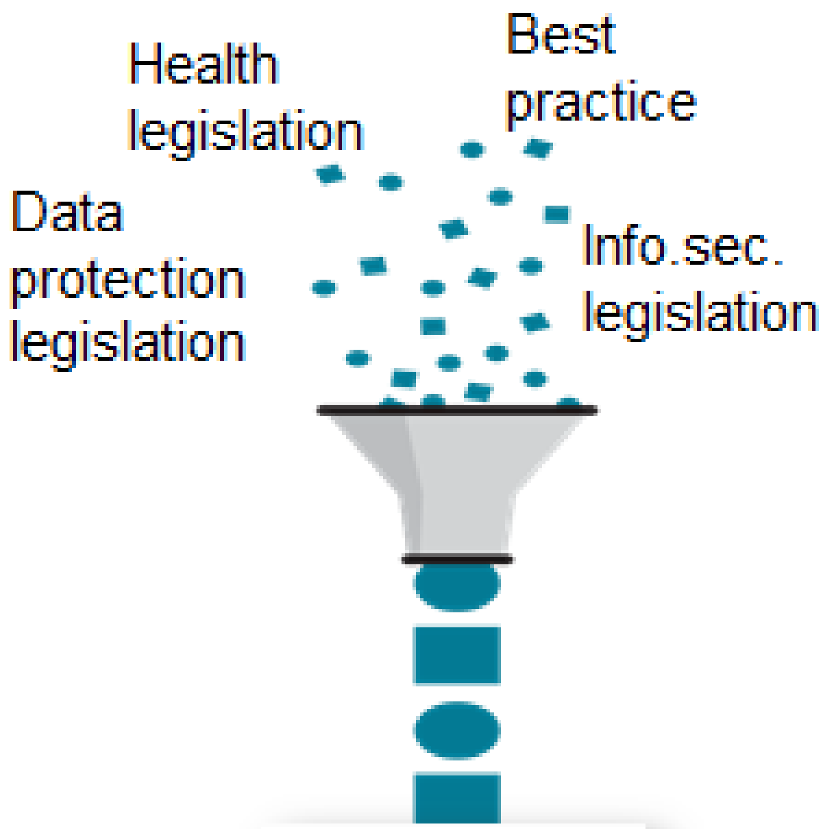
Direktoratet for e-helse

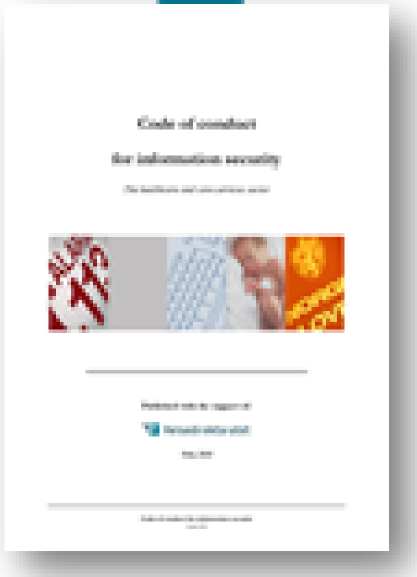
Norwegian health network and HealthCERT

- Secure telecommunications network developed and managed by the government
- Provide the most efficient and secure electronic exchange of patient information possible between all relevant parties within the health and social services sector
- Essentially a set of VPNs
- Most healthcare organizations are connected
- 700.000 electronic messages are sent through the health network every day and rapidly increasing
- Code of conduct – end to
- HealthCERT - shares knowledge about ICT threats and protection mechanisms, and continuously monitors traffic within the health network
- The national protection program

Background

- Extensive health and care sector
- Organizationally fragmented
- Sensitive personal data
- Electronic exchange of information
- Complicated legislation




Code of conduct

for information security

2006 – Version 1.0

Managed and developed

- Developed and managed by a steering committee with representatives from the health and care services sector
- Secretariat at the Directorate for e-Health together with resources from Norwegian Health Network
- Workshops
- Sector-wide participation

Government

Public service providers

Professional associations/ Trade unions

Legislative authorities

The Code of conduct

Binding –
affiliation agreement with
Norwegian Health Network

Norm

for informasjonssikkerhet

Helse-, omsorgs- og sosialsektoren

Utgitt med støtte av:

Helsedirektoratet

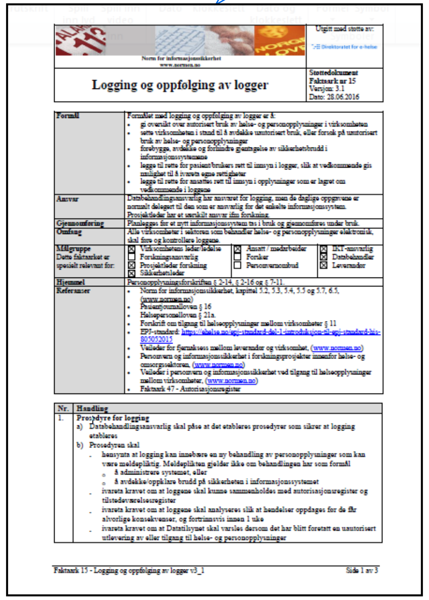
Oslo, 2018

Norm for informasjonssikkerhet

The Code and some of the guidelines are translated to english

Guidelines
Factsheets (best practice routines)

Not binding

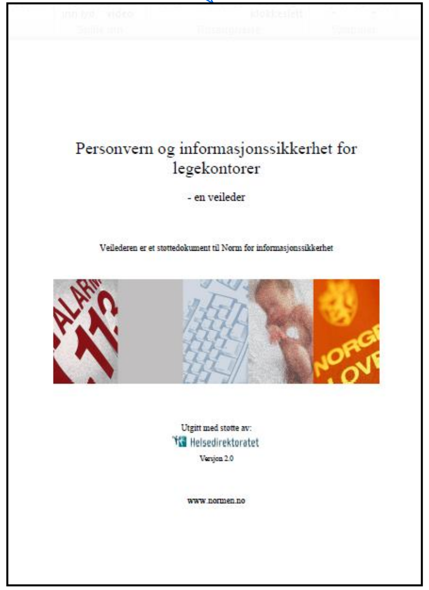


Norm for informasjonssikkerhet www.normen.no	Utgitt med støtte av: Direktoratet for e-helse
Logging og oppfølging av logger	**Støttedokument** **Faktaark nr 15** Versjon: 3.1 Dato: 28.06.2016

Formål	Formålet med logging og oppfølging av logger er å: • gi oversikt over autorisert bruk av helse- og personopplysninger i virksomheten • sette virksomheten i stand til å avdekke uautorisert bruk, eller forsøk på uautorisert bruk av helse- og personopplysninger • forebygge, avdekke og forhindre gjentagelse av sikkerhetsbrudd i informasjonssystemene • legge til rette for pasient/brukers rett til innsyn i logger, slik at vedkommende gis mulighet til å ivareta egne rettigheter • legge til rette for ansattes rett til innsyn i opplysninger som er lagret om vedkommende i loggene		
Ansvar	Databehandlingsansvarlig har ansvaret for logging, men de daglige oppgavene er normalt delegert til den som er ansvarlig for det enkelte informasjonssystem. Prosjektleder har et særskilt ansvar ifm forskning.		
Gjennomføring	Planlegges før et nytt informasjonssystem tas i bruk og gjennomføres under bruk.		
Omfang	Alle virksomheter i sektoren som behandler helse- og personopplysninger elektronisk, skal føre og kontrollere loggene.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig ☒ Prosjektleder forskning ☒ Sikkerhetsleder	☒ Ansatt / medarbeider ☐ Forsker ☐ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☒ Leverandør
Hjemmel	Personopplysningsforskriften § 2-14, § 2-16 og § 7-11.		
Referanser	• Norm for informasjonssikkerhet, kapittel 5.2, 5.3, 5.4, 5.5 og 5.7, 6.5, (www.normen.no) • Pasientjournalloven § 16 • Helsepersonelloven § 21a. • Forskrift om tilgang til helseopplysninger mellom virksomheter § 11 • EPJ-standard: https://ehelse.no/epj-standard-del-1-introduksjon-til-epj-standard-his-805052015 • Veileder for fjernaksess mellom leverandør og virksomhet, (www.normen.no) • Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren, (www.normen.no) • Veileder i personvern og informasjonssikkerhet ved tilgang til helseopplysninger mellom virksomheter, (www.normen.no) • Faktaark 47 - Autorisasjonsregister		

Nr.	Handling
1.	**Prosedyre for logging** a) Databehandlingsansvarlig skal påse at det etableres prosedyrer som sikrer at logging etableres b) Prosedyren skal - hensynta at logging kan innebære en ny behandling av personopplysninger som kan være meldepliktig. Meldeplikten gjelder ikke om behandlingen har som formål ○ å administrere systemet, eller ○ å avdekke/oppklare brudd på sikkerheten i informasjonssystemet - ivareta kravet om at loggene skal kunne sammenholdes med autorisasjonsregister og tilstedeværelsesregister - ivareta kravet om at loggene skal analyseres slik at hendelser oppdages før de får alvorlige konsekvenser, og fortrinnsvis innen 1 uke - ivareta kravet om at Datatilsynet skal varsles dersom det har blitt foretatt en uautorisert utlevering av eller tilgang til helse- og personopplysninger

Faktaark 15 - Logging og oppfølging av logger v3_1 Side 1 av 3



Personvern og informasjonssikkerhet for legekontorer

- en veileder

Veilederen er et støttedokument til Norm for informasjonssikkerhet

Utgitt med støtte av:
Helsedirektoratet
Versjon 2.0

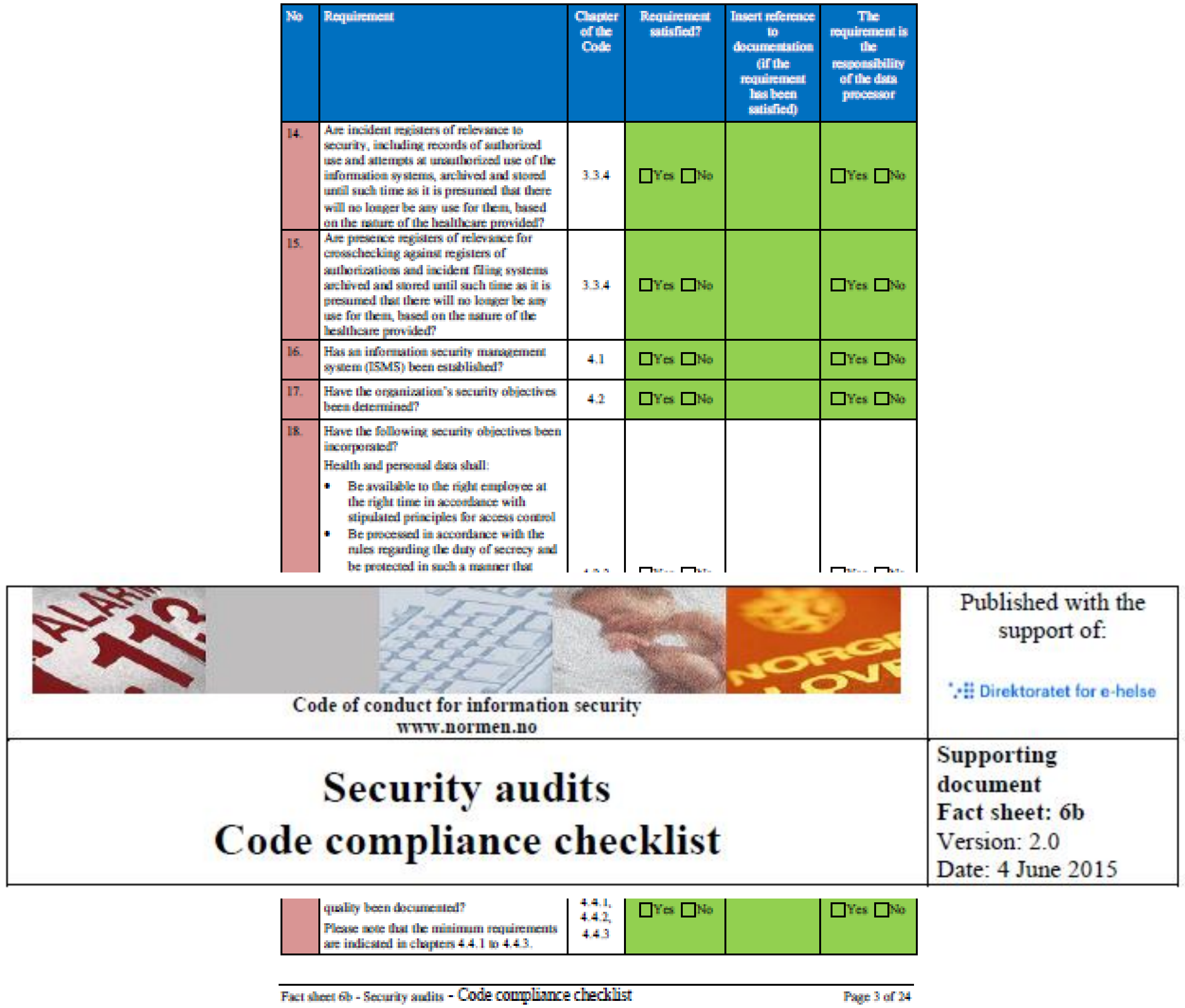
www.normen.no

Direktoratet for e-helse

Examples - guidelines and factsheets

- Guideline for remote access between supplier and organization *
- Guideline for privacy and information security in medical devices
- Fact sheet 6b: Security audits - Code compliance checklist *
- Guideline and template for general practitioners and physicians in private practice.
- Guidelines for social media
- Factsheet 42: Use of SMS for patient contact *

- * available in English



No	Requirement	Chapter of the Code	Requirement satisfied?	Insert reference to documentation (if the requirement has been satisfied)	The requirement is the responsibility of the data processor
14.	Are incident registers of relevance to security, including records of authorized use and attempts at unauthorized use of the information systems, archived and stored until such time as it is presumed that there will no longer be any use for them, based on the nature of the healthcare provided?	3.3.4	☐Yes ☐No		☐Yes ☐No
15.	Are presence registers of relevance for crosschecking against registers of authorizations and incident filing systems archived and stored until such time as it is presumed that there will no longer be any use for them, based on the nature of the healthcare provided?	3.3.4	☐Yes ☐No		☐Yes ☐No
16.	Has an information security management system (ISMS) been established?	4.1	☐Yes ☐No		☐Yes ☐No
17.	Have the organization's security objectives been determined?	4.2	☐Yes ☐No		☐Yes ☐No
18.	Have the following security objectives been incorporated? Health and personal data shall: • Be available to the right employee at the right time in accordance with stipulated principles for access control • Be processed in accordance with the rules regarding the duty of secrecy and be protected in such a manner that				
	quality been documented? Please note that the minimum requirements are indicated in chapters 4.4.1 to 4.4.3.	4.4.1, 4.4.2, 4.4.3	☐Yes ☐No		☐Yes ☐No

Fact sheet 6b - Security audits - Code compliance checklist Page 3 of 24

Code of conduct for information security
www.normen.no

Published with the support of:
Direktoratet for e-helse

Security audits
Code compliance checklist

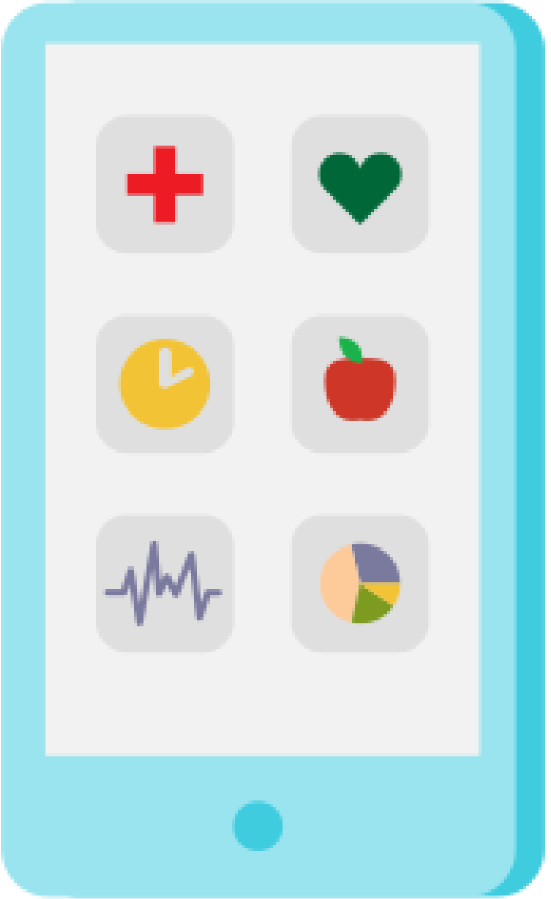
Supporting document
Fact sheet: 6b
Version: 2.0
Date: 4 June 2015

Why has the Code been a success?

- Binding by contract
- Non-bureaucratic – “bottom up”
- The stakeholders are involved
- Practical advices
- Sector specific guidance
- An arena for information security and privacy questions
- In partnership with the legislative authorities
- Financed by the government
- Simplifies, and makes complicated regulation more accessible

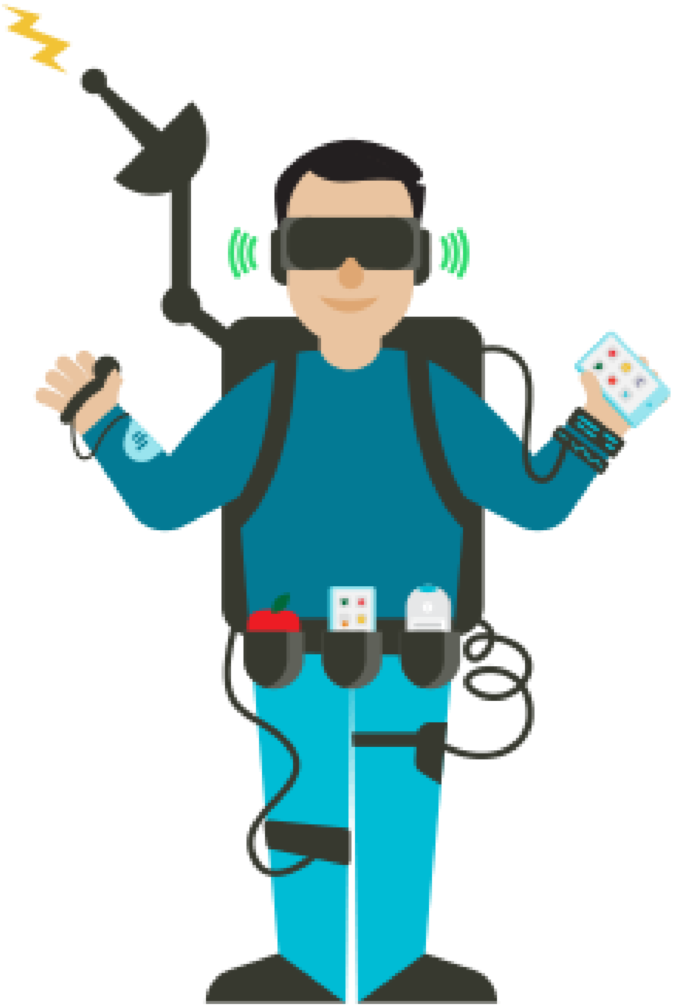
Best of…. 2016

- Cloud computing
- Guideline on joint EMR
- Guideline on Personal Connected Health and Care services
- Factsheet – Malicious code
- Concept for an security awareness program in the health sector

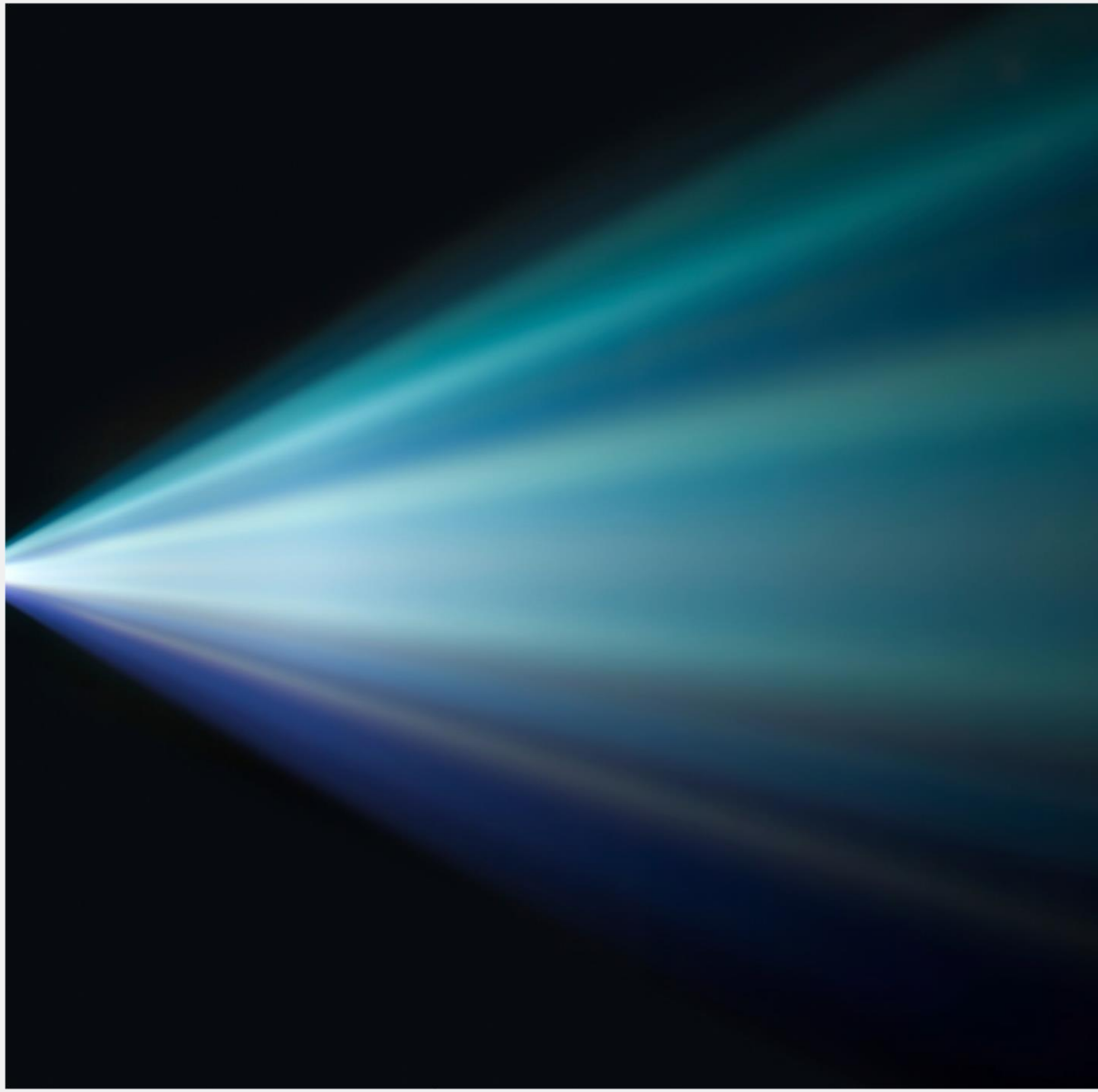


Focus 2017

- EU data protection reform – GDPR
- Secondary use and health registries
- Personal Connected Health and Care services
- Videoconference for clincial use
- Information security requirements for medical devices
- ~~Th~~e code of conduct vs ISO27001 Annex A
- Training and design
- Education – colleges and universities



Guidelines for Cloud computing in the healthsector



Direktoratet for e-helse

Background

- Increased interest in Cloud Computing
- Complicated legal framework for processing outside of Norway
- Data Protection Authority involved in cases relating to municipalities use of Cloud Computing fo sensitive personal data
- Increased focus on cost efficiency
- On-going work with a national strategy for tl of Cloud Computing within the public sector

Cloud Computing Strategy for Norway

- The main objective is to provide public and private enterprises with more room for manoeuvre when deciding which ICT solutions to use.
- The strategy should facilitate:
  - more cost-effective ICT solutions
  - increased focus on core activities
  - greater flexibility
  - greater security through more professional and standardised ICT
  - lower threshold for innovation and startups
  - reduced carbon footprint from ICT operations
- https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

Circular on digitization for 2016

- Issued to all public agencies, included the principle for using cloud computing:
- Cloud computing shall be assessed on the same basis as other solutions when considering major changes or reorganisation of ICT systems or operations:
  - when procuring new systems or performing major upgrades
  - when undertaking extensive replacements of hardware
  - when existing operating agreements expire
- When they offer the most appropriate and cost-effective solution and when no particular obstacles stand in the way of using them, **cloud services should be chosen.**
- The chosen solution must satisfy the agency’s requirements for **information security**. This means that enterprises must **know the value** of its own systems and data, and perform a **risk assessment** of the chosen solution.

Sector involvement

- Working group with a sector-wide participation;
  - hospitals
  - municipalities
  - vendors/ suppliers
  - Norwegian Health Network
  - Directorate for Public Management and eGovernment
  - Data Protection Authority
  - University of Oslo

Aim and Scope

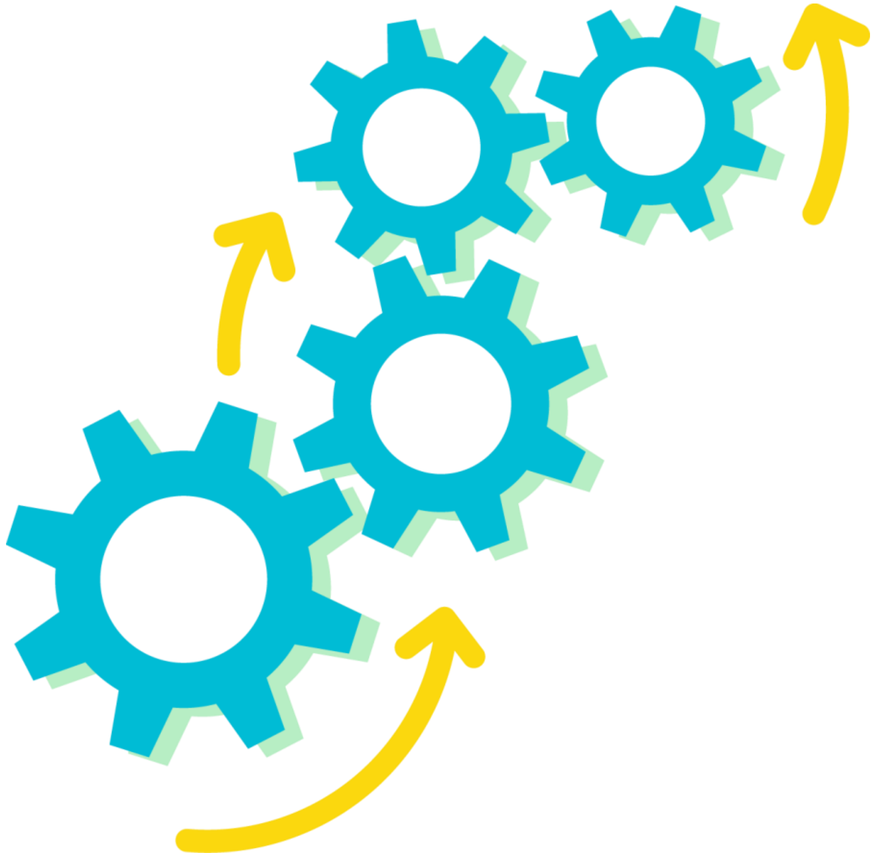
- Provide guidelines for secure use of Cloud Computing wihtin the health and care sector
- Demystifying the Cloud
- Life-cycle perspective; planning, procuring, negotiating, setting-up, managing and terminating

Main Focus

- Demystifying the cloud
- What is the cloud?
- Which kind of services can be provided?
- Risks in the Cloud
- Benefits of Cloud computing

Main Focus

- Legal perspective
- Duties of the data controller
- Contracts
- Rights of the data subjects
- Transfer to EU/EEA and third countries
- Information security
  - Access control
  - Logging
  - Encryption
  - Configuration control



Main challenges

- Different needs and level of understanding within the target groups
- Legal premises
  - Safe Harbour/ Privacy Shield
  - Norwegian laws on public archives did not allow storage of archive material outside of Norway
  - Relatively strict data protection legislation and practice in Norway

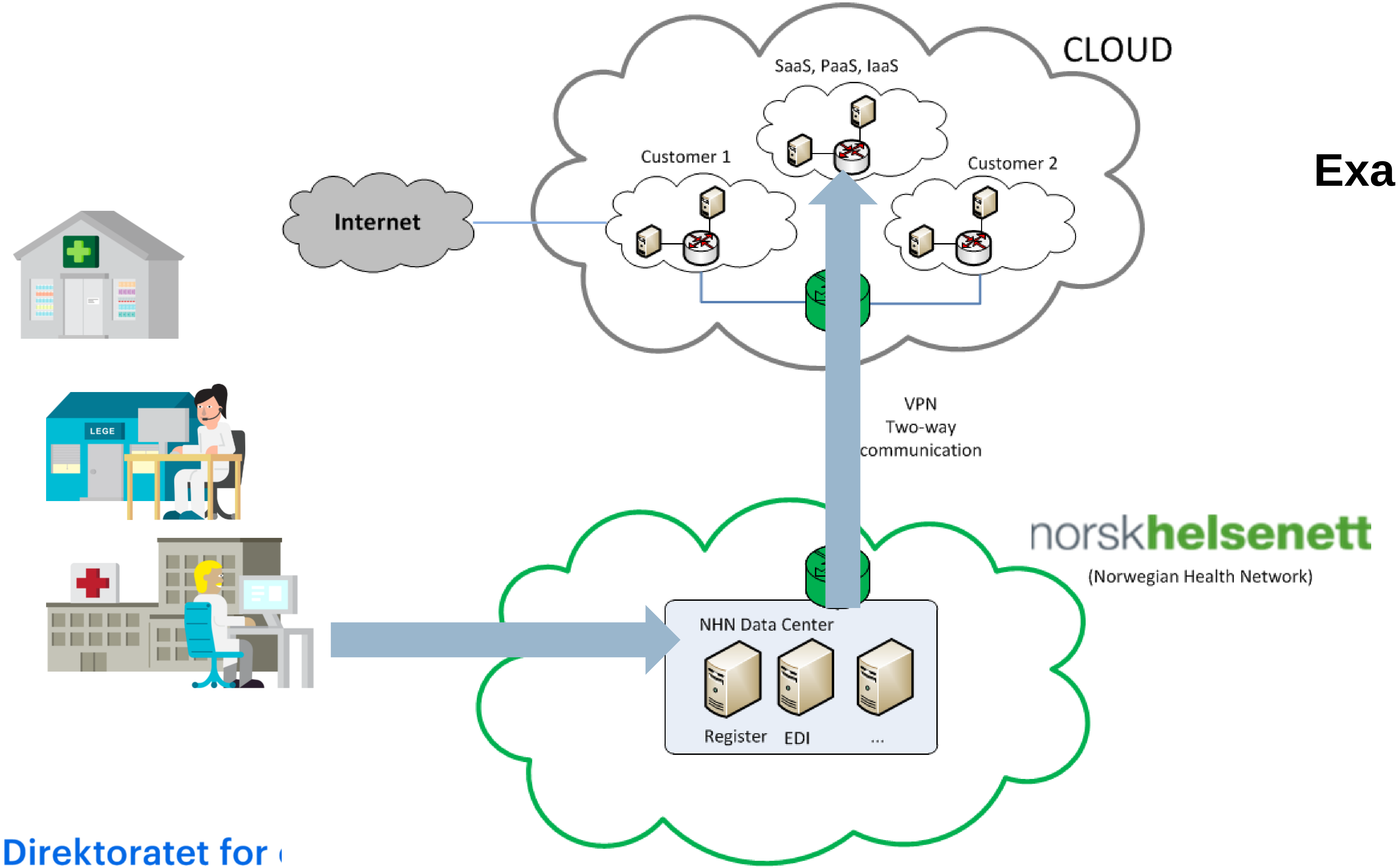
Example: Cloud services for health Information - work in progress by Norwegian Health Network

- Nearly **all health care providers in Norway are connected** to the Norwegian Health Network, and approx.150 **third-party service providers**

- They receive **weekly requests** on how to connect to cloud services through their infrastructure

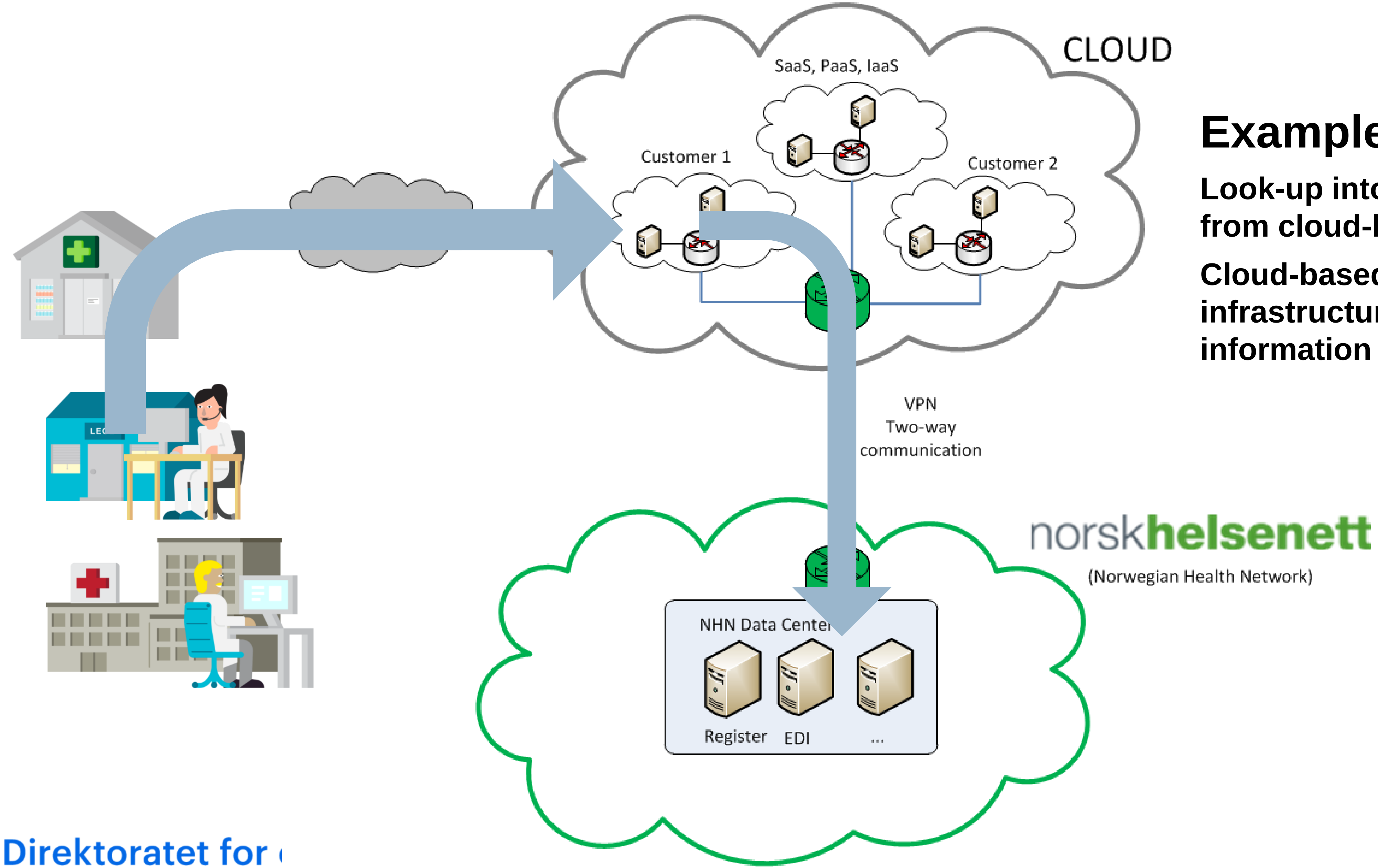
- A procurement process is coming up (techology-neutral)
- First cloud provider is directly connected to the health network.
  - Security based on virtual zoning and virtual routing controlled by the Norwegian Health Network. (Azure: ExpressRoute Circuit)
  - More cloud providers to come

Use case 1: Consuming cloud services from the Health Network



Example: Data analysis, BI

Use case 2: Consuming Health Network services from the cloud



Examples:

Look-up into The National EDI address register from cloud-based EPR-systems

Cloud-based EPR-systems using EDI infrastructure in the Health Network for health information exchange

Direktoratet for
e-helse

Thank you!

sikkerhetsnormen@ehelse.no
#normen / @Normen_no
www.normen.no
www.ehelse.no