



Direktoratet for
e-helse

Norwegian Code of conduct for information security in the health and care sector

eHealthweek Amsterdam 8.6.16

Aasta M. Hetland, Norwegian Directorate of eHealth

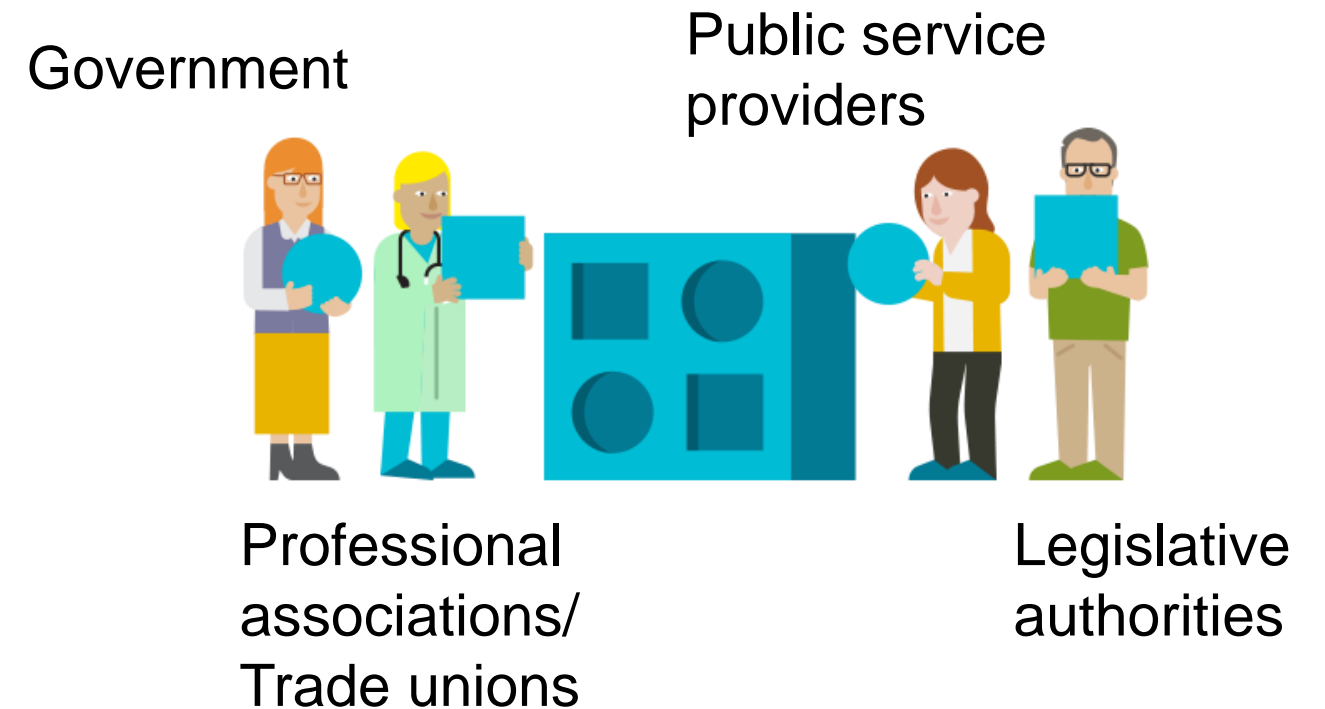
Background

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



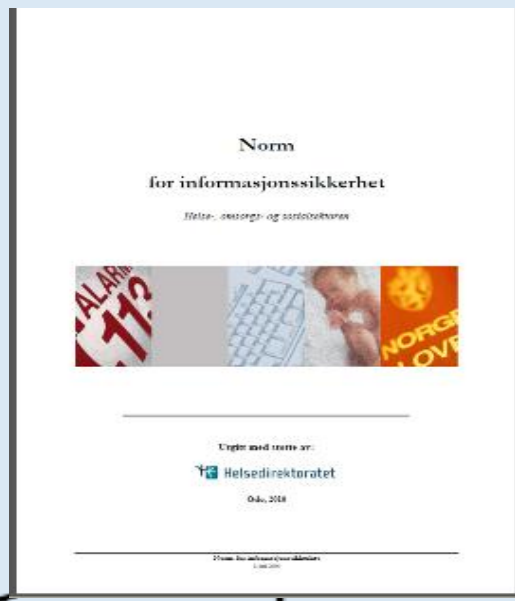
Managed and developed

- 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 with representatives from the sector and with people outside the sector who have relevant input
- Sector-wide participation in other activities



The Code of conduct

*Binding –
affiliation agreement with
Norwegian Health Network*



The Code and some of the guidelines are translated to english

- Guidelines
- Factsheets (best practice routines)



Not binding

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	<input type="checkbox"/> Yes <input type="checkbox"/> No		<input type="checkbox"/> Yes <input type="checkbox"/> 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	<input type="checkbox"/> Yes <input type="checkbox"/> No		<input type="checkbox"/> Yes <input type="checkbox"/> No
16.	Has an information security management system (ISMS) been established?	4.1	<input type="checkbox"/> Yes <input type="checkbox"/> No		<input type="checkbox"/> Yes <input type="checkbox"/> No
17.	Have the organization's security objectives been determined?	4.2	<input type="checkbox"/> Yes <input type="checkbox"/> No		<input type="checkbox"/> Yes <input type="checkbox"/> No
18.	Have the following security objectives been incorporated? Health and personal data shall: <ul style="list-style-type: none"> • 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 				



Published with the support of:


Code of conduct for information security
www.normen.no

Security audits
Code compliance checklist

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

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	<input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Yes <input type="checkbox"/> No
---	---------------------------	--	--

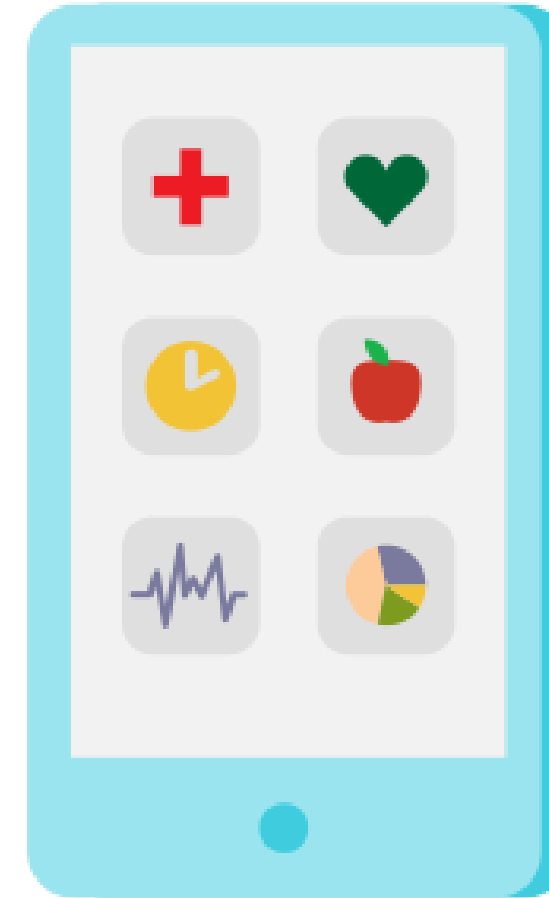
Why has the Code been a success?

- Binding by contract
- The timing was right
- Non-bureaucratic – “bottom up”
- The stakeholders are involved
- Up-to-date on relevant topics
- Practical advices
- Sector specific guidance
- An arena for information security and privacy questions
- In partnership with the legislative authorities
- Financed by the government
- Low budget – high value
- Simplifies, and makes complicated regulation more accessible



Focus 2016

- Cloud computing
- Guideline on joint EHR
- Guideline on Welfare technology
- Concept for security awareness program
- Education – colleges and universities



Other activities

Annual conference



Trondheim
11. – 12.oktober

Newsletter



- 4 times per year
- Subscribe at www.normen.no

Q&A email

sikkerhetsnormen@ehelse.no

Training and talks



- Training
- Conferences
- Lectures and talks

www.normen.no



- The documents
- News
- Training
- Etc.

Twitter

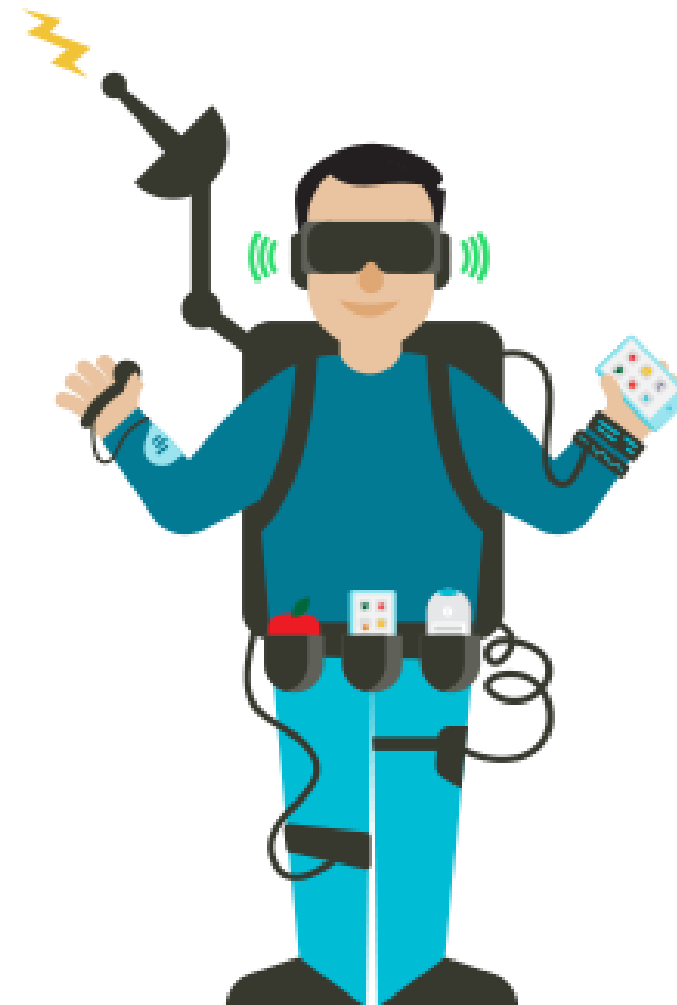


[@Normen_no](https://twitter.com/Normen_no)



Going forward

- Telemedicine
- EU data protection reform - GDPR
- Training, monitoring and use
- Modernize design and form
- Establish Nordic and European contacts





Direktoratet for
e-helse

Thank you!

sikkerhetsnormen@ehelse.no

[#normen](#) / [@Normen_no](#)

www.normen.no

www.ehelse.no