NORMEN

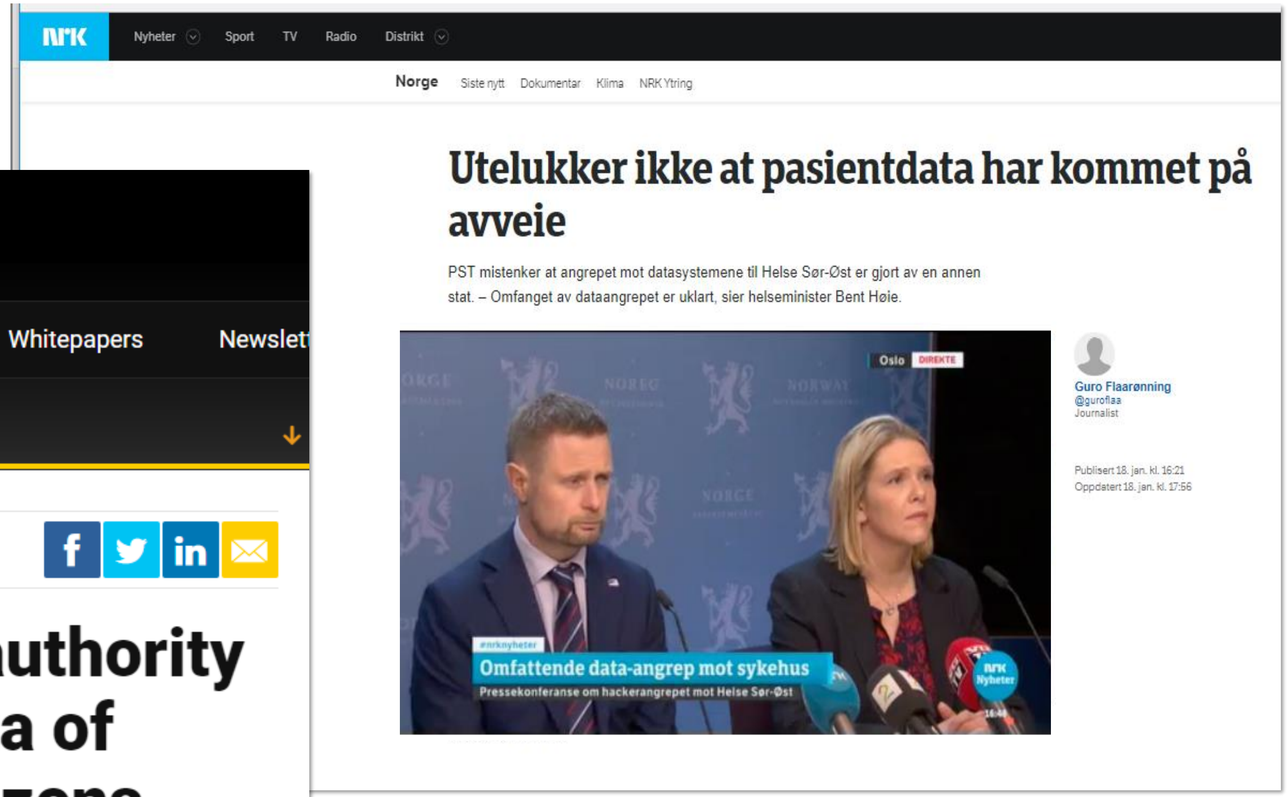
Normens veileder for Informasjonssikkerhet og personvern - medisinsk utstyr

Kurs i informasjonssikkerhet basert på Normen for medisinsk-teknisk personell

13. februar 2020

Bakgrunn

Målrettet cyber-angrep mot Helse Sør-Øst



NORMEN

Ny teknologi - nye utfordringer

- Skyen, apper, bigdata…
- Lange og komplekse digitale verdikjeder
  - Der også pasientens / brukerens eget utstyr /apper inngår
- Vanskelige risikovurderinger
- Forventninger fra pasienter og pårørende

U.S. Department of Health and Human Services

U.S. Food and Drug Administration
Protecting and Promoting *Your* Health

A to Z Index | Follow FDA | En Español

Search FDA

Home | Food | Drugs | Medical Devices | Radiation-Emitting Products | Vaccines, Blood & Biologics | Animal & Veterinary | Cosmetics | Tobacco Products

Medical Devices

Home > Medical Devices > Medical Device Safety > Safety Communications

Safety Communications

- Information About Heparin
- Preventing Tubing and Luer Misconnections

Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

SHARE | TWEET | LINKEDIN | PIN IT | EMAIL | PRINT

Date Issued: July 31, 2015

Audience: Health care facilities using the Hospira Symbiq Infusion System

Device: Symbiq Infusion System, Version 3.13 and prior versions

The Hospira Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population.

It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

Purpose:

The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that health care facilities transition to alternative infusion systems, and discontinue

NORMEN

Conficker i Helse Vest 2009

https://www.nrk.no/rogaland/helse-data — NORSK RIKSKRINGKA... — cyber attacks on medical devic... — Medical devices at risk from cy... — Helse-datavirus kjent siden ...

Norm for informasjonssik... — http--eur-lex.europa — Fjerntilgang — Google — Masterkatalog for Normd... — 360 - Hjem — analytics — Fazer Food Services AS- F... — LINK — MinTid — Samhandlingsportalen til ...

nrk — Nyheter — Sport — TV — Radio — Distrikt

Rogaland TV Radio 84/85 Retro Tips oss!

Tre måneder gammelt virus slo ut Helse Vest

Andre institusjoner har gått klar, men Helse Vest fikk sirup-pc-er.

Mari Rollag Evensen
@mariroll

Publisert 13.01.2009, kl. 07:19

Downadup, eller Conficker, ble første gang oppdaget i IT-verdenen i oktober 2008. Microsoft sendte samme måned ut en sikkerhetsoppdatering som skulle stoppe virusets muligheter til å ødelegge. (Illustrasjonsfoto)
FOTO: ILLUSTRASJONSFOTO: COLOURBOX

Tirsdag 5. januar ble mange av de 25.000 ansatte i Helse Vest møtt av dataviruset Downadup da de kom på jobb. **Ormen, som har rammet helseregionen i én uke, ble imidlertid oppdaget i oktober 2008.**

Viruset har foreløpig ikke gjort at personopplysninger har kommet på

DN Dagens Næringsliv — Oslo Børs: 15:28 Indeks: 693,77 +0,19%

DN Investor. Overvåk markedet med skreddersydd

Tekno Teknologi

Helse Vest slått ut av datavirus

Sykehus på hele Vestlandet har i flere dager vært rammet av det verste dataviruset på åtte år.

NTB
Publisert: 08.01.2009 – 07:49 Oppdatert: 07.02.2014 – 06:36

NORMEN

Dagbladet

30.04.18

SÅRBARE: Røntgenmaskiner, spesielt med gammel programvare, er sårbare for malware-angrep. Foto: ded pixto / Shutterstock / NTB Scanpix

Hacker seg inn på røntgen- og MR-maskiner. Også Norge rammet

Ny gruppe pekes ut.

NORMEN

Noen kjente hendelser knyttet til MU og informasjonssikkerhet…

«GE-saken»

DAGENS Medisin

Leder: Vi skal være glade for prioriterings-dilemmaene

Nyheter | Debatt | Blogger | Leder | Legeliv | DM-Quiz | DM-TV | Jobbmarkedet | DM Arena | Annon

Siste nytt | Helsepolitikk | Forskning | Kreft | Hjerte og kar | Legemidler | Folkehelse | Livsstil | Psykisk helse

Oppdatert 28.03.12 *Nyheter*

Tok personopplysninger fra 126.344 nordmenn

GE Healthcare System hentet ulovlig ut sensitiv informasjon om 126.344 pasienter som ledd i overvåking av røntgenutstyr. Datatilsynet har nå tatt affære overfor de aktuelle sykehusene og røntgeninstituttene.

Personvernnemnda

Forside | Regelverk | Vedtak | Klage | Om PVN | Mer om personvern | Søk

Alle
2014
2013
2012
2011
2010

Datatilsynets referanse: 12/00297-8/BSO

PVN-2013-11 Oslo universitetssykehus

Klage på Datatilsynets vedtak om pålegg – uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang

Personvernnemndas avgjørelse av 20. desember 2013 (Eva I. E. Jarbekk, Arve Føyen, Ørnulf Rasmussen, Gisle Hannemyr, Marta Ebbing, Ann R Sætnan)

The Guardian

International edition

Hacking risk leads to recall of 500,000 pacemakers due to patient death fears

FDA overseeing crucial firmware update in US to patch security holes and prevent hijacking of pacemakers implanted in half a million people

▲ Abbott / St Jude Medical's Accent MRI pacemaker, one of the affected devices that had to be recalled. Photograph: Abbott / St Jude Medical

Almost half a million pacemakers have been recalled by the US Food and Drug Administration (FDA) due to fears that their lax cybersecurity could be hacked to run the batteries down or even alter the patient's heartbeat.

The recall won't see the pacemakers removed, which would be an invasive and dangerous medical procedure for the 465,000 people who have them implanted: instead, the manufacturer has issued a firmware update which

TECHNOLOGY FOX NEWS

Search foxnews.com

TECH HOME COMPUTERS GOOGLE VIDEO GAMES MILITARY TECH WAR GAMES SLIDESHOWS

SECURITY

US government probes for possible cyber flaws

Published October 22, 2014 · Reuters

Jay Radcliffe shows off a Medtronic Corp insulin pump at his home in Meridian, Idaho. (CYBERSECURITY-MEDICALDEVICES/ REUTERS/Brian Losness)

The U.S. Department of Homeland Security is investigating about two do cases of suspected cybersecurity flaws in medical devices and hospital equipment that officials fear could be exploited by hackers, a senior offic agency told Reuters.

Fighting for the Right to Open his Heart Data: Hugo (TEDxCambridge 2011

TEDx Talks

Abonner 4 053 523

DN.no

MAGASINET

Magasinet Teknologi

De medisinske hackerne

Da sikkerhetseksperten Marie Moe (37) fikk hjerteproblemer, oppdaget hun at det er mulig å hac livskritiske, medisinske apparater som pacemakere, morfinpumper og insulinutstyr.

Tekst: Osman Kibar Foto: Maxim Sergienko
Publisert: 08.01.2016 — 21:28

Les hele magasinet

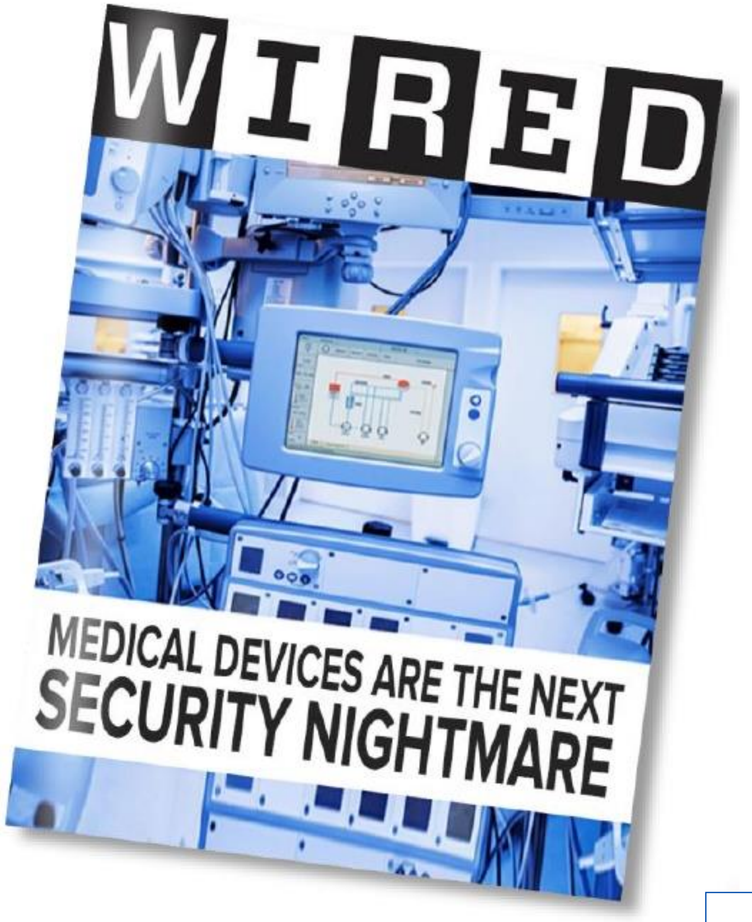
- Det er en grunn til at USAs visepresident Dick Cheney fikk fjernet den trådløse enheten i den implanterte hjertestarteren sin, sier Sintef-forsker og sikkerhetsekspert Marie Moe.

Cheneys kardiolog fryktet et attentatforsøk gjennom hacking av enheten. Da Moe selv fikk operert inn en pacemaker, oppdaget hun at den hadde egenskaper ingen hadde fortalt henne om.

NORMEN

Medisinsk utstyr og informasjonssikkerhet – hva er problemet?

- Fra stand-alone til hyper-konnektivitet (IoT)
- Svak endepunkt-sikkerhet
- Kjente sårbarheter eksisterer
- Kan utnyttes som brohode som «svakeste ledd»
- Gap i forvaltning
  - Organisatorisk
  - Kompetanse
  - Metodikk (safety vs security)



Medisinsk utstyr
– definisjon etter forskrift om håndtering av medisinsk utstyr

Ethvert instrument, apparat, utstyr, **programvare**, materiale eller annen gjenstand som brukes alene eller i kombinasjon, **herunder programvare** som av produsenten er tiltenkt å brukes spesielt til diagnostiske og/eller terapeutiske formål (…)

kompensasjon for skade eller handikap,

3. undersøkelse, utskifting eller endring av anatomien eller av en fysiologisk prosess, eller

4. svangerskapsforebyggelse,

og der den ønskede hovedvirkning i eller på menneskekroppen ikke framkalles ved farmakologisk eller immunologisk virkning eller ved å påvirke stoffskiftet, men der slike effekter kan bidra til dets funksjon.

NORMEN

Kompetansekrav og samtykke

Forskrift om elektroforetak og kvalifikasjonskrav for arbeid knyttet til elektriske anlegg og elektrisk utstyr - §8

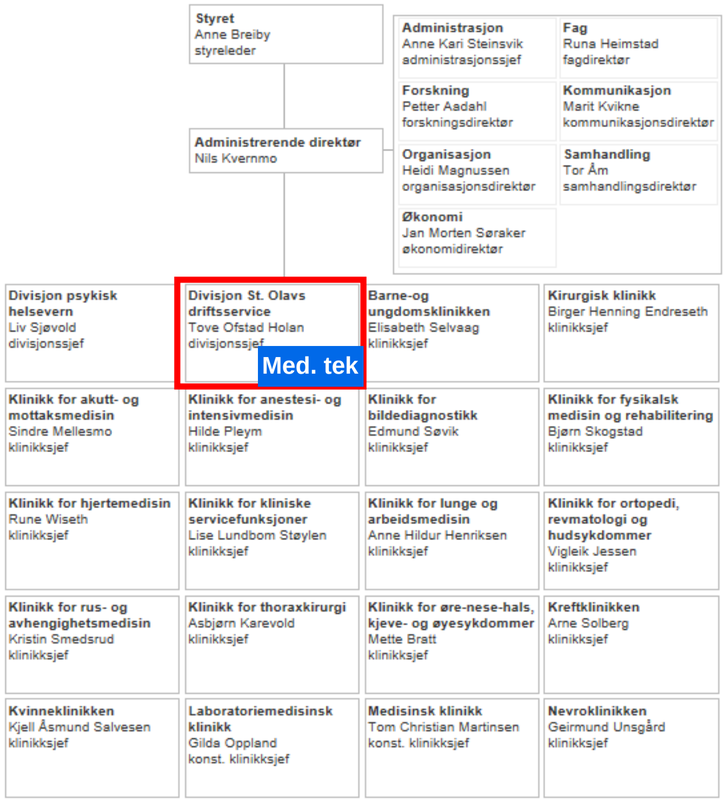
(…)

Den som har det faglige ansvaret for og den som reparerer elektromedisinsk utstyr klasse IIa, IIb og III, skal ha utdanning som dataelektroniker, master- eller bachelorgrad eller toårig fagskole innen elektronikk eller utdanning som gir tilsvarende relevant elektrokompetanse. Vedkommende skal ha tre års relevant praksis (…)

Vedkommende skal ha samtykke fra Direktoratet for samfunnssikkerhet og beredskap eller fra den direktoratet bemyndiger.

Organisering av medisinsk-tekniske avdelinger vs. IKT

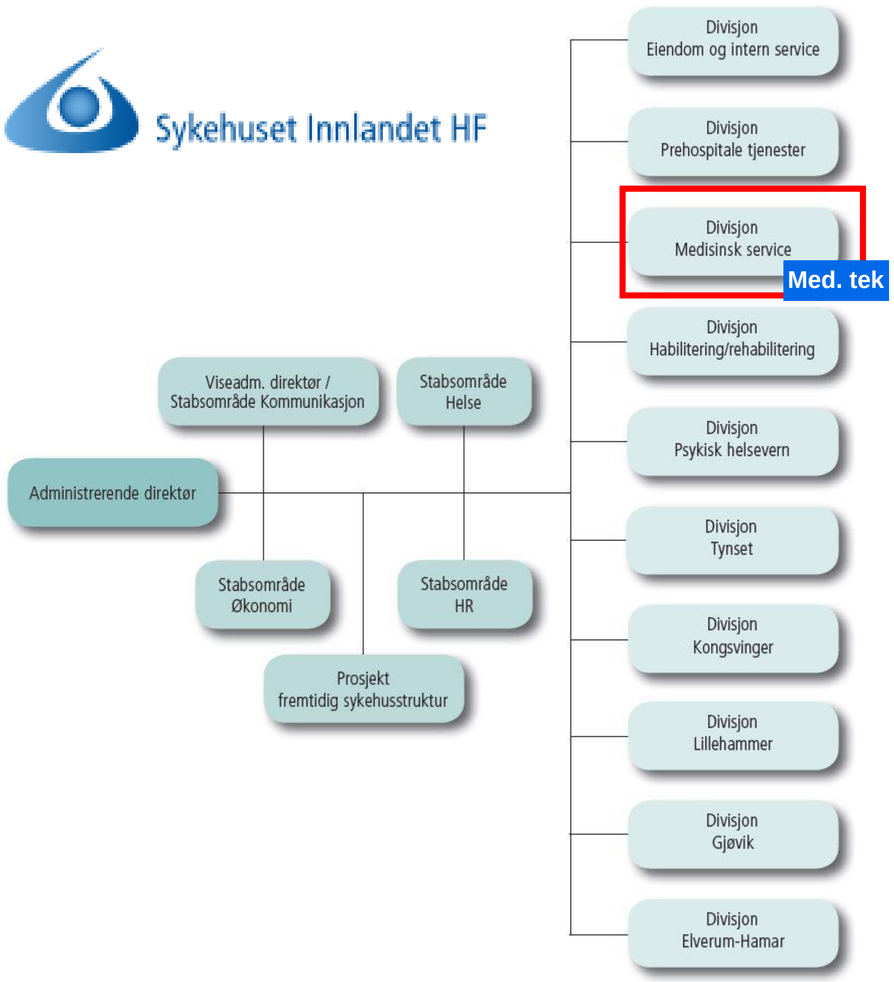
ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM



HELSE MIDT-NORGE IT

NORMEN

Organisering av medisinsk-tekniske avdelinger vs. IKT



SYKEHUSPARTNER

NORMEN

Før:

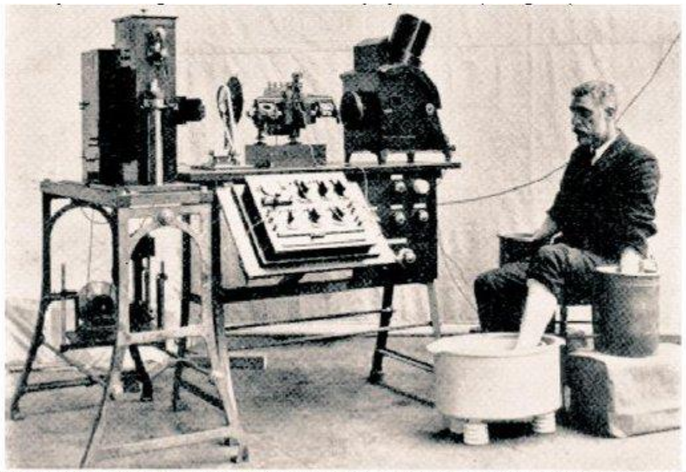


Fig. 6. The first table-model Einthoven electrocardiograph manufactured by the Cambridge Scientific Instrument Company of London in 1911. On the right hand side the arch lamp, in the centre on the table the string galvanometer, and below the switching board for the leads, next left to the camera the timer (rotating wheel with spokes), and on the left hand side the falling-plate camera (from Burch, De Pasquale, A History of Electrocardiography p 33 [14]).

- Stand-alone utstyr hvor operatør måtte oppsøke utstyret for å gjøre endringer og avlese verdier
- Liten eller ingen mulighet for brukertilpasninger

Nå:

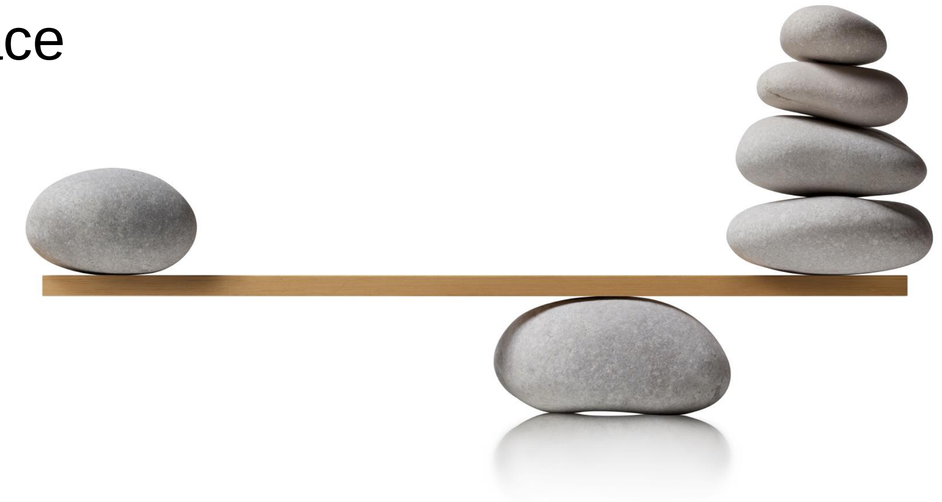
- «Alt» er tilkoblet nettverk
- Måleresultater og innstillinger overføres til sentrale servere/applikasjoner
- Muligheter for brukertilpasset menyer, alarmer, bilder osv.
- Sikkerhetsfunksjoner for å unngå feilbehandling.

Klinisk beste løsning – eller løsning som støtter best integrasjon og sikkerhet?

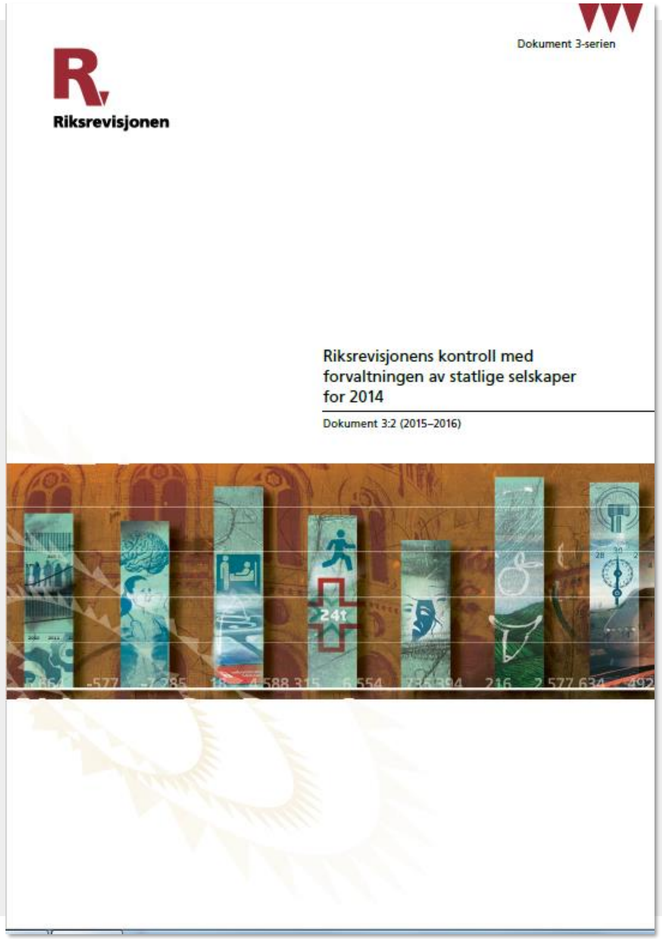
- Legen sier: «**Klinisk beste løsning!»**

Men:

- Leverandøren leverer ikke HL7 eller DICOM interface
- Leverandøren støtter lagring, men kun filshare
- Pålogging, ingen støtte for dette
- Må være lokal-administrator på PC
- Hendelseslogg – viser til Windows logg
- Antivirus – ikke tale om!
- Sikkerhetspatchinger av OS – kun fra leverandør



Riksrevisjonens selskapskontroll 2014



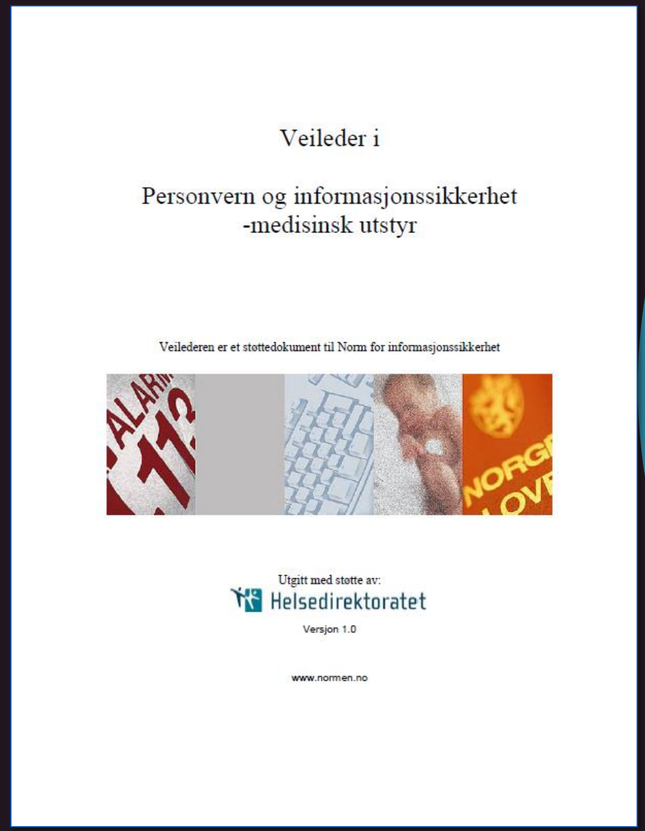
Sak 3: Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr

Hovedfunn:

- Helseforetakene stiller ikke tilstrekkelige krav om informasjonssikkerhet i avtaler med leverandører av medisinsk-teknisk utstyr og har mangelfull oppfølging av leverandører.
- Helseforetakene har mangelfull oversikt over risiko knyttet til informasjonssikkerhet i medisinsk-teknisk utstyr.
- Det er uklare ansvarslinjer for informasjonssikkerhet i medisinsk-teknisk utstyr internt i helseforetakene og mellom helseforetakene og de regionale it-enhetene.

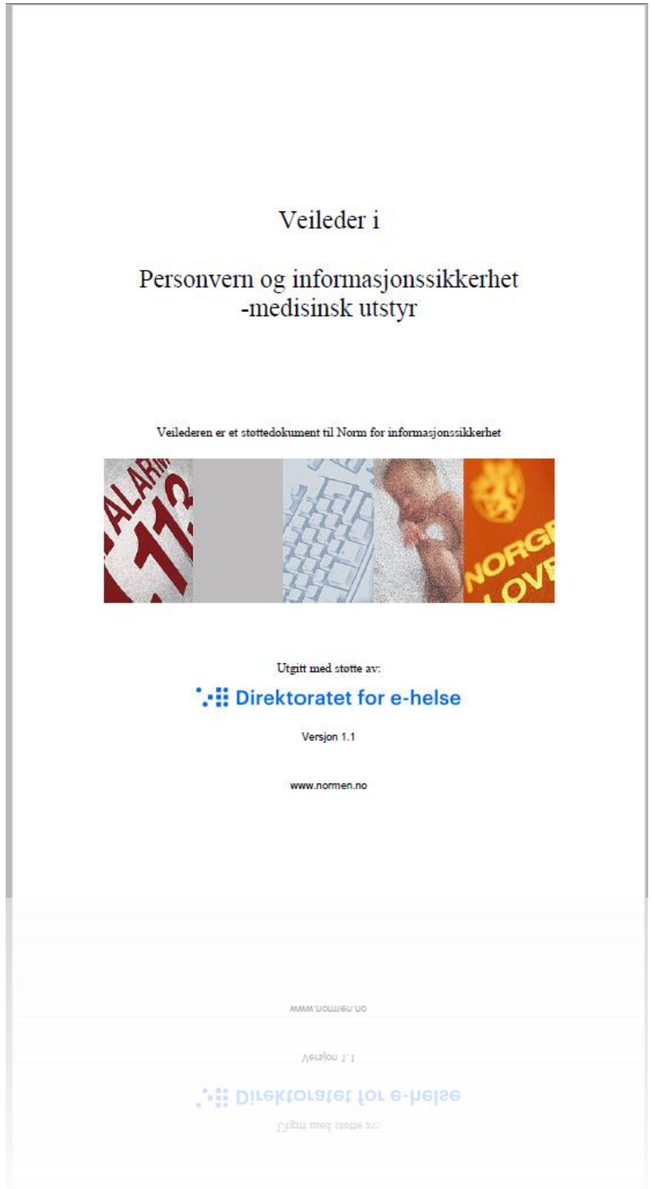
NORMEN

Veileder i
Personvern og informasjonssikkerhet
- medisinsk utstyr



Normens arbeid med informasjonssikkerhet og medisinsk utstyr

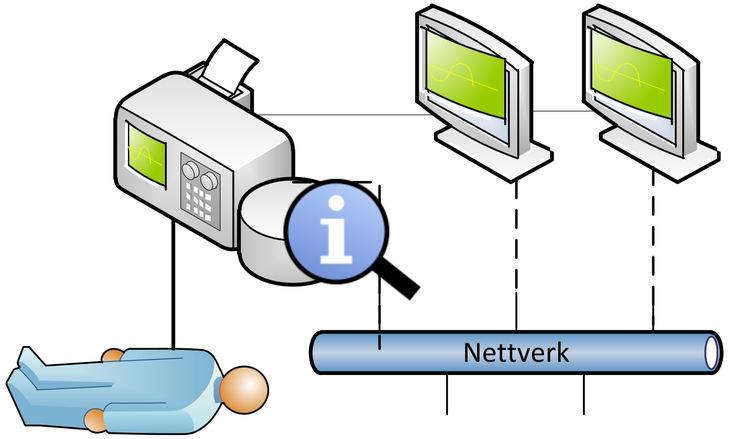
- Publiserte veileder desember 2015
- Deltakere i referansegruppen fra AHUS, Datatilsynet, DSB, Helse Bergen, Helse Sør-Øst, Helsedirektoratet, Helse Vest IKT, HEMIT, St. Olavs Hospital, Stavanger universitetssjukehus, Sykehuset Telemark, Sykehuset Østfold, Vingmed AS / Medtek Norge.
- Revidert versjon 2017: Tatt inn lenke til generiske krav ved anskaffelser
- 2017: Kurs for alle helseregioner basert på veilederen
- 2018-2019: Arrangert åpent kurs
- 2020: Skal revidere scenarier



NORMEN

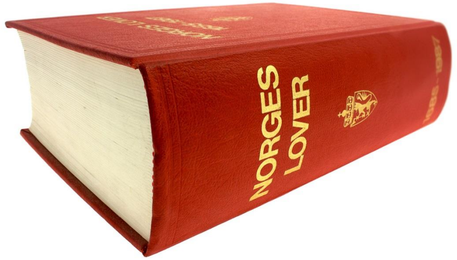
Veileder i
Personvern og informasjonssikkerhet - medisinsk utstyr

- Veilederen skal bidra til å skape **felles forståelse** for **krav og tilnærming til informasjonssikkerhet** hos
  - Virksomheter som benytter MU
  - Databehandlere
  - Leverandører av medisinsk utstyr
- Veilederen finnes her: https://ehelse.no/veileder-i-personvern-og-informasjonssikkerhet-medisinsk-utstyr

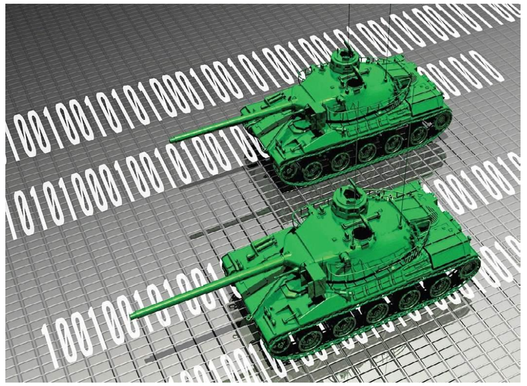


Hovedtemaer i veilederen:

- Hvordan sikre at behandling av helse- og personopplysninger i tilknytning til medisinsk utstyr skjer i tråd med lovverket

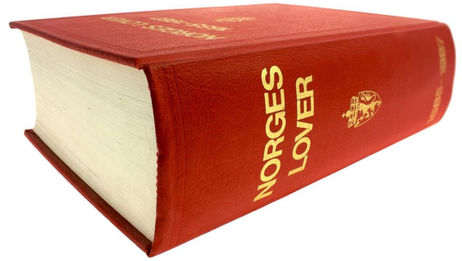


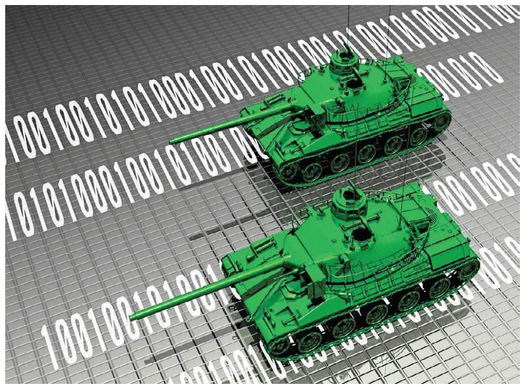
- Hvordan medisinsk utstyr kan beskyttes mot angrep på digital infrastruktur



Hovedmomenter

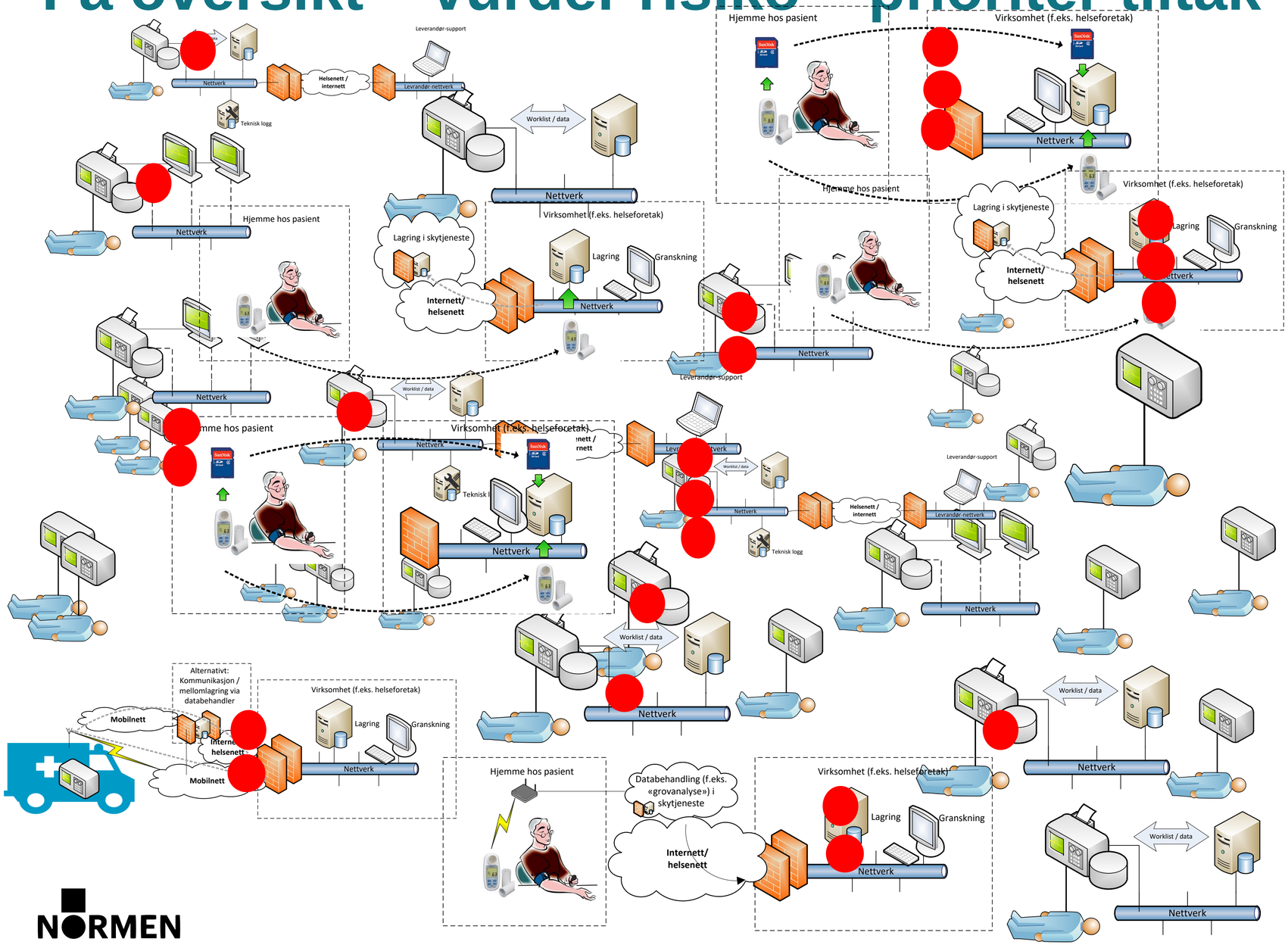
- To hovedtemaer i veilederen:
  - Hvordan sikre at behandling av helse- og personopplysninger i tilknytning til medisinsk utstyr skjer i tråd med lovverket
  - Hvordan medisinsk utstyr kan beskyttes mot angrep på digital infrastruktur





- Utfordring:
  - I vurderingen av sikkerhetstiltak for medisinsk utstyr, vil eventuell påvirkning på funksjon og bruk av utstyret måtte tillegges stor vekt
- Tilnærming:
  - Forholdsmessighet i valg av tiltak
  - Risikobasert

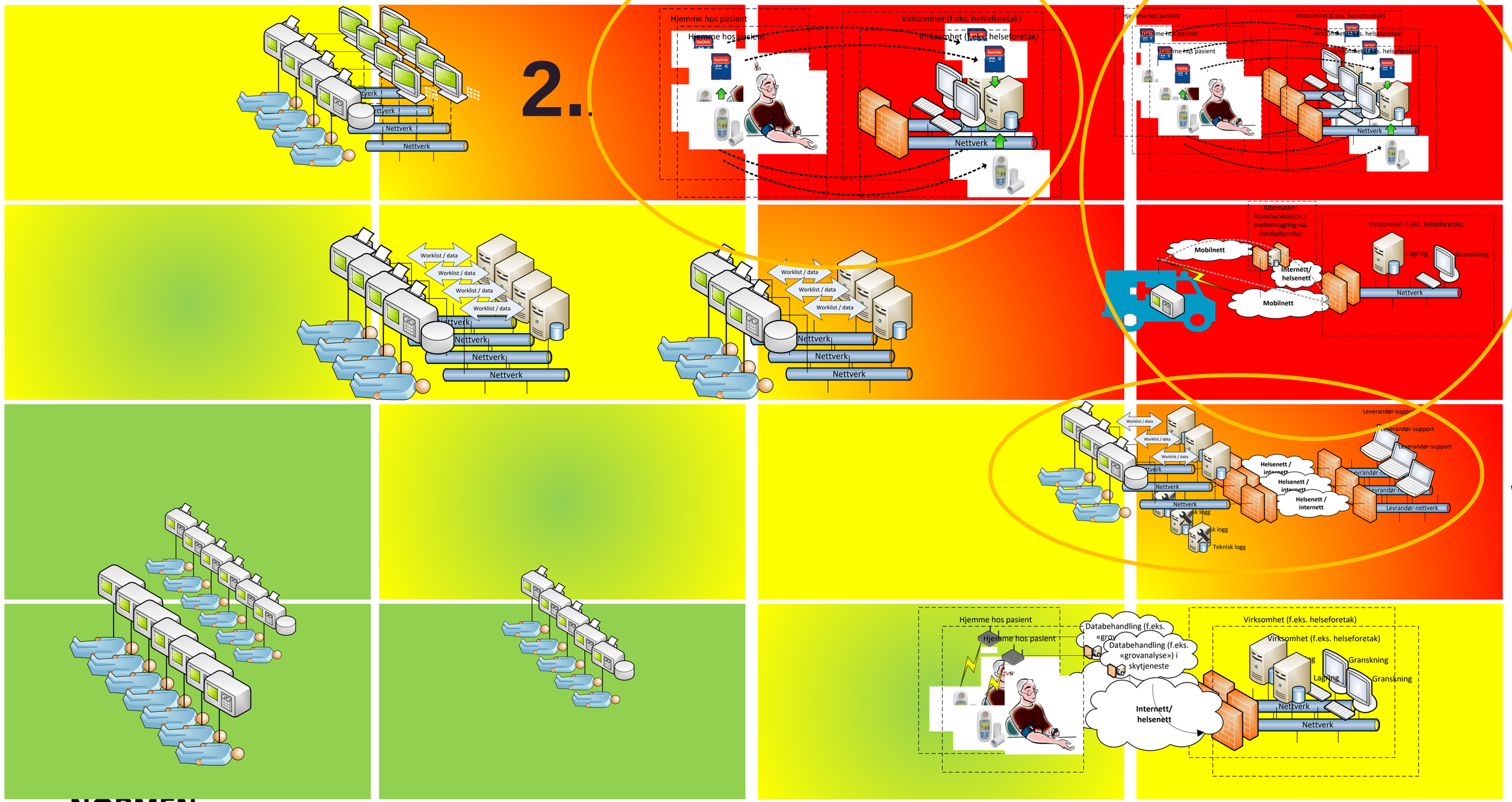
Få oversikt – vurder risiko – prioriter tiltak



Eksempler på spørsmål til hjelp for å kategorisere løsningene:

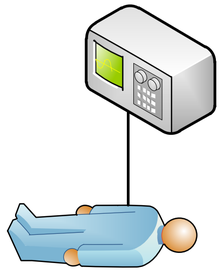
- Behandles pasientidentifiserbare data?
- Er utstyret nettverkstilknyttet?
- Har leverandør tilgang via VPN?

Få oversikt – vurder risiko – prioriter tiltak



Bruksscenarier

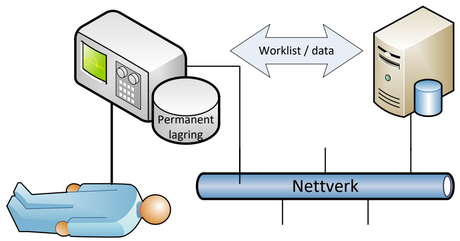
2. Frittstående MU uten lagring.



Delområde	
Behandling av helse- og personopplysninger	Ja
Direkte identifiserbare helse- og personopplysninger	Ja
Avidentifiserte helse- og personopplysninger	Nei
Overføring av data i lokale nettverk	Nei
Overføring av data i eksterne nettverk	Nei
Teknisk overvåkning	Nei
Leverandørtilknytning	Nei
Trådløs kommunikasjon	Nei
Intern lagring	Nei
Ekstern lagring (f.eks. DVD)	Nei
Serverbasert lagring	Nei
Databehandler / skyløsning	Nei
Hvem har konfigurasjonskontroll	Virksomheten

...

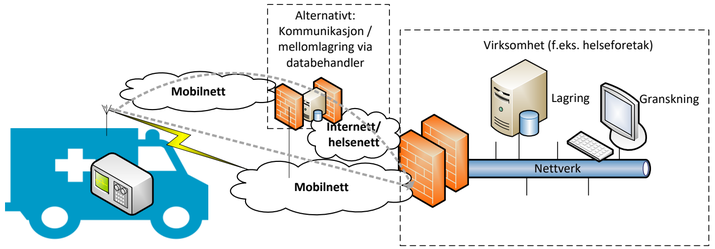
8. Nettverkstilkoplet MU som lagrer data/rapport både eksternt og internt.



Delområde	
Behandling av helse- og personopplysninger	Ja
Direkte identifiserbare helse- og personopplysninger	Ja
Avidentifiserte helse- og personopplysninger	Nei
Overføring av data i lokale nettverk	Ja
Overføring av data i eksterne nettverk	Nei
Teknisk overvåkning	Nei
Leverandørtilknytning	Nei
Trådløs kommunikasjon	Nei
Intern lagring	Ja, permanent
Ekstern lagring (f.eks. DVD)	Nei
Serverbasert lagring	Ja
Databehandler / skyløsning	Nei
Hvem har konfigurasjonskontroll	Virksomheten

...

11. MU som overfører data via mobilnettverk (f.eks. fra ambulanser)



Delområde	
Behandling av helse- og personopplysninger	Ja
Direkte identifiserbare helse- og personopplysninger	Ja
Avidentifiserte helse- og personopplysninger	Nei
Overføring av data i lokale nettverk	Ja
Overføring av data i eksterne nettverk	Ja
Teknisk overvåkning	Nei
Leverandørtilknytning	Nei
Trådløs kommunikasjon	Ja
Intern lagring	Ja
Ekstern lagring (f.eks. DVD)	Nei
Serverbasert lagring	Ja
Databehandler / skyløsning	Kan
Hvem har konfigurasjonskontroll	Kan være leverandør

Eksempel på bruksscenario: Nettverkstilkoplet MU som lagrer data/rapport både eksternt og internt, med leverandørtilgang

Tilstrekkelig sikring mot innsyn fra uvedkommende
Fysisk sikring (4.6)

Tilgangsstyring (kap 4.8) og *hendelsesregistrering* (4.9) på sentralt utstyr

Nettverkssikkerhet, sikkerhets-oppdateringer og tiltak mot skadelig kode (4.10)

Sikkerhetstiltak ved datalagring (4.7)

Sikring av leverandørtilgang (4.5.3 og egen veileder)

Regulere konfigurasjonskontroll gjennom avtale (Normen kap. 5.5.1)

Kontroll på hvilke data som overføres til tekniske logger, sikring av logger

Eksempel: MR.
Rådata og bilder blir lagret lokalt mens bilder også lagres eksternt.
Tekniske data overføres til en teknisk logg til bruk i feilsøking og systemadministrasjon.
Leverandør/produsent trenger VPN-tilgang til utstyret for å drive f.eks. driftsovervåking

1. Alle i gruppa finner en type medisinsk utstyr / system man kjenner godt til

2. Behandles pasientidentifiserbare data?
3. Er utstyret nettverkstilknyttet?
4. Har leverandør tilgang via VPN?

5. Diskuter i fellesskap hvilke av bruksscenariene som best beskriver utstyret

Mulig metodikk for risikovurdering: IEC 80001 Application of risk management for IT-networks incorporating medical devices

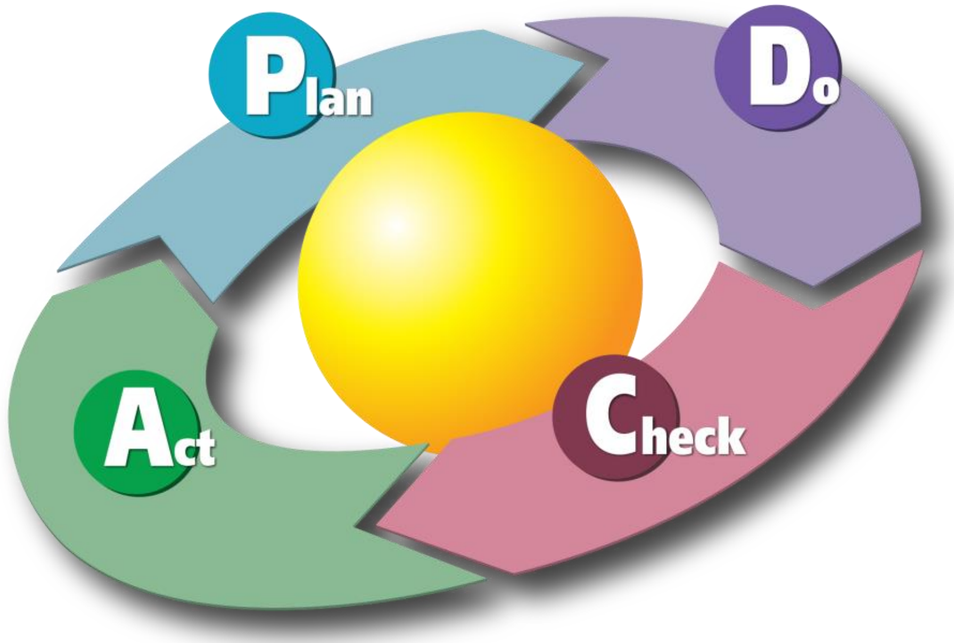
- Roller, ansvar og aktiviteter når medisinsk utstyr tilknyttes virksomhetens IT-nettverk
- Tre «Key properties» skal adresseres i risikostyringen:
  - «Safety» (tilsvarende trygghet / sikkerhet som brukt i konteksten HMS eller pasientsikkerhet)
  - «Effectiveness» (evne til å skape ønsket resultat for pasient og virksomheten)
  - «Data and system security» (tilsvarende informasjonssikkerhet)
- Viktig rolle: «Medical it-network risk manager»
- Beskriver risikostyring gjennom endringsstyring i livsløpsperspektiv for medisinske IT-nettverk

Basis sikkerhetstiltak

- Ivareta den registrertes rettigheter
  - Taushetsplikt
  - Behandlingsgrunnlag
  - Innsynsrett
  - Retting og sletting
- Databehandlingsansvarlig
- Opplæring og kompetanse
- Kravstilling ved anskaffelser
- Service og support fysisk hos virksomheten
  - Taushetserklæringer han håndteres av leverandøren

Inkludere MU i styringssystem for informasjonssikkerhet

- Beskrive roller og ansvar
  - Delta på felles arenaer
- Inkludere leverandører og systemer i oversikter
- Avtaler
- Inkludere i den gjennomførende delen
- Inkludere i den kontrollerende delen
  - Avvik
  - Sikkerhetsrevisjoner
  - Risikovurderinger
  - Ledelsens gjennomgang

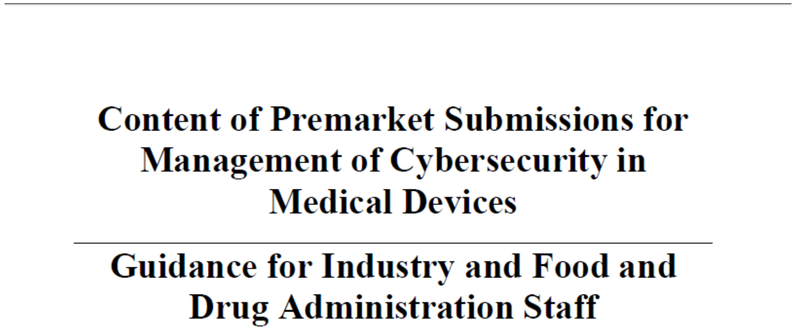


Sikkerhetstiltak ved behov (risikoavhengig)

- Tiltak ved fjernsupport
- Bruk av databehandler
  - Databehandleravtale når leverandør behandler data
  - Innsyn i helse- og personopplysninger utløser i seg selv ikke behov for databehandleravtale (men taushetserklæring)
- Fysisk sikring
- Tilgangsstyring
- Hendelsesregistrering
- Nettverkssikkerhet og tiltak mot skadelig kode
- Skytjenester
- Tilgang til helseopplysninger utover virksomhetsgrenser
- Utlevering av helseopplysninger til utlandet

Nettverkssikkerhet og tiltak mot skadelig kode

- Vanlige tiltak:
  - Anti-virus programvare
  - Programvareoppdateringer
  - Ikke tildel sluttbrukere administrator-rettigheter
  - Blokker kjøring av ikke-autoriserte programmer («hvitelisting»)
- Segmentere MU på dedikerte nettverk
  - Skadelig kode kan fortsatt infisere via f.eks. minnepenner


Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

- Still krav til leverandøren om å dokumentere hvordan cyber-sikkerhet ivaretas for utstyret i hele utstyrets levetid
- Krav til kodesignatur for programvare oppdateringer
- Mulighet for sikkerhetsmonitorering MU
- Informasjon til sluttbruker om handling ved mistanke om sikkerhetsbrudd
- «Fail-safe» modus ved digitale angrep
- Mulighet for autorisert bruker å rulle tilbake opprinnelig konfigurasjon


don't let
PERFECT
be the enemy
of the
GOOD.

Regulation on medical devices (MDR) – Annex 1
Safety and performance requirements related to cybersecurity

- 17.1. Devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, shall be designed to **ensure repeatability, reliability and performance in line with their intended use. In the event of a single fault condition, appropriate means shall be adopted to eliminate or reduce as far as possible consequent risks or impairment of performance.**

- 17.2. For devices that incorporate software or for software that are devices in themselves, **the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security,** verification and validation.

- 17.4. **Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.**

- 24.4 The instructions for use shall contain all of the following particulars:(ab) for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves**, minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.**

NORMEN

Spørsmål?