Medisinsk utstyr og informasjonssikkerhet

Geir-Erlend Myhre Johansen
Jan Gunnar Broch, Direktoratet for e-helse/ Sekretariatet for Normen

Webinar 7.april 2021

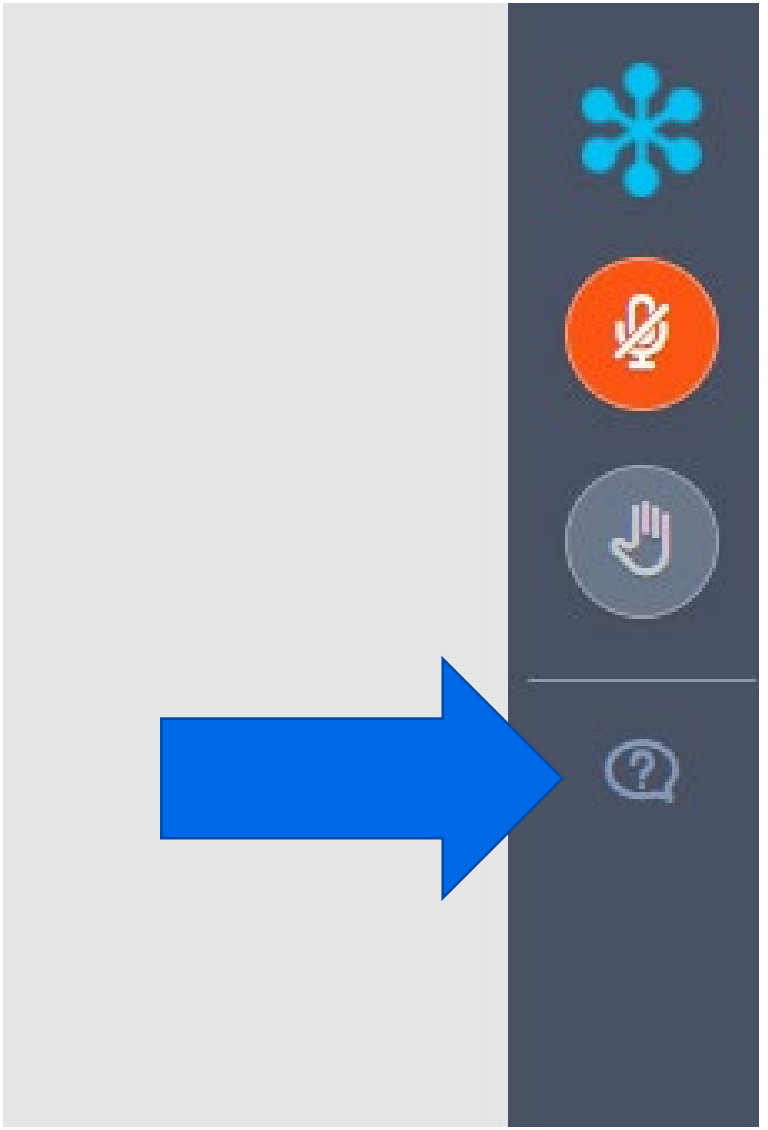
Kjøreregler

- Møteleder styrer ordet
- Deltagernes mikrofoner er mutet som standardinnstilling
- Det foretas ikke opptak av dette webinaret
- Deaktiver fullskjermsmodus dersom du har problemer med å svare på poll
- Presentasjonene legges ut på kurssiden på normen.no

- Vil du vite mer om hvordan vi jobber med GoToWebinar? Se mer på https://ehelse.no/normen/aktuelt-om-normen/digital-kompetanseheving-med-normen

Spørsmål underveis

- Bruk spørsmålsfunksjonen når som helst under foredragene
- Vi svarer på spørsmål enten i plenum og/eller i chat
- Vi lagrer spørsmålet ditt, men ikke hvem det kommer fra
- Hvis du har spørsmål som ikke blir besvart under kurset, send oss en epost til sikkerhetsnormen@ehelse.no



Agenda

- Problemstillinger knyttet til MU og sikkerhet
  v/ Geir-Erlend Myhre Johansen,
  St. Olavs hospital

- Status fra Normen om medisinsk utstyr og informasjonssikkerhet
  v/ Jan Gunnar Broch
  Sekretariatet for Normen

- Innsendte spørsmål og diskusjon

POLL

Problemstillinger knyttet til MU og sikkerhet

Geir-Erlend Myhre Johansen
IKT-koordinator MTA
St. Olavs Hospital

St. Olavs driftsservice

ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

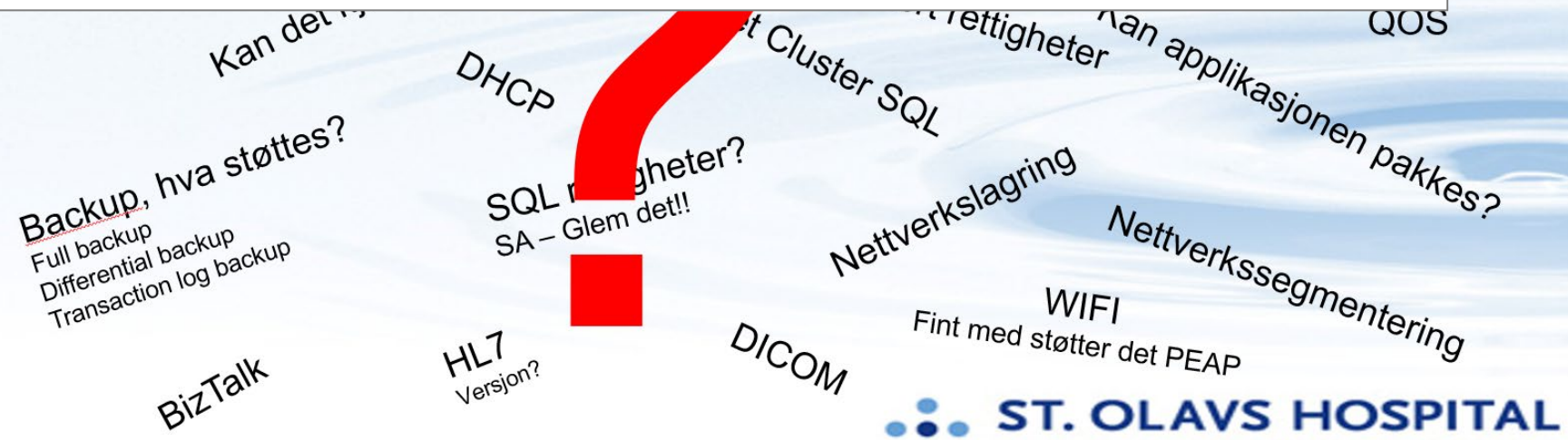
Fra min presentasjon på Bransjetreff til Medtek Norge 2016

Nytt apparat og programvare som skal på nett
Ja vel……

Nytt apparat og programvare som skal på nett
Ja vel……

Personvernforordningen

GDPR



ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

St. Olavs driftsservice

St. Olavs driftsservice

Er det med sikkerhet så viktig da? Vi er da ikke noe mål!

Aftenposten A-magasinet Osloby Sport Meninger Søk Meny

Verden | Datasikkerhet

Sensitive personopplysninger fra psykoterapisenter på avveie. Nå presses pasienter for penger.

Søndag holder den finske regjeringen krisemøte om skandalen som vokser i omfang.

WEBINA
Please

Ransomware has come a long way since the first attack at an international AIDS conference, where each victim had to pay $189 to regain access to their computer. Now, hackers are demanding higher ransoms from healthcare organizations that have more to lose.

Last month, Hancock Health, a healthcare network in Indiana, paid hackers $55,000 in ransom to unlock its systems. Previously, the California-based Center for Orthopedic Specialists (COS) and Hawaii's Fetal Diagnostic Institute of the Pacific were both hit by ransomware attacks, potentially leaking the data of more than 100,000 patients.

>> READ: WannaCry Virus Attack Stresses Healthcare's Need to Fortify Defenses

St. Olavs driftsservice

«Men det er MTU…. Det kan ikke patches – det går jo på pasientsikkerheten…»

- Man vil aldri oppnå god pasientsikkerhet uten en god IT-sikkerhet.

- Det hjelper så lite med en robust og bra MTU-applikasjon som kjører på et utdatert OS.

St. Olavs driftsservice

ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

«Og forresten så kan ikke MTU patche…. pga. sertifisering»

U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993
FDA.GOV

U.S. FOOD & DRUG ADMINISTRATION

FDA FACT SHEET

THE FDA'S ROLE IN MEDICAL DEVICE CYBERSECURITY

Dispelling Myths and Understanding Facts

Dispelling the Myths	Understanding the Facts
The FDA is the only federal government agency responsible for the cybersecurity of medical devices.	The FDA works closely with several federal government agencies including the U.S. Department of Homeland Security (DHS), members of the private sector, medical device manufacturers, health care delivery organizations, security researchers, and end users to increase the security of the U.S. critical cyber infrastructure.
Cybersecurity for medical devices is optional.	Medical device manufacturers must comply with federal regulations. Part of those regulations, called quality system regulations (QSRs), requires that medical device manufacturers address risks, including cybersecurity risk. The pre- and post- market cybersecurity guidances provide recommendations for meeting QSRs.
Medical device manufacturers can't update medical devices for cybersecurity.	Medical device manufacturers can always update a medical device for cybersecurity. In fact, the FDA does not typically need to review changes made to medical devices solely to strengthen cybersecurity

ST. OLAVS driftsservice

ITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

Kilde: https://www.fda.gov/media/123052/download

MDR

Nye forordninger om medisinsk utstyr

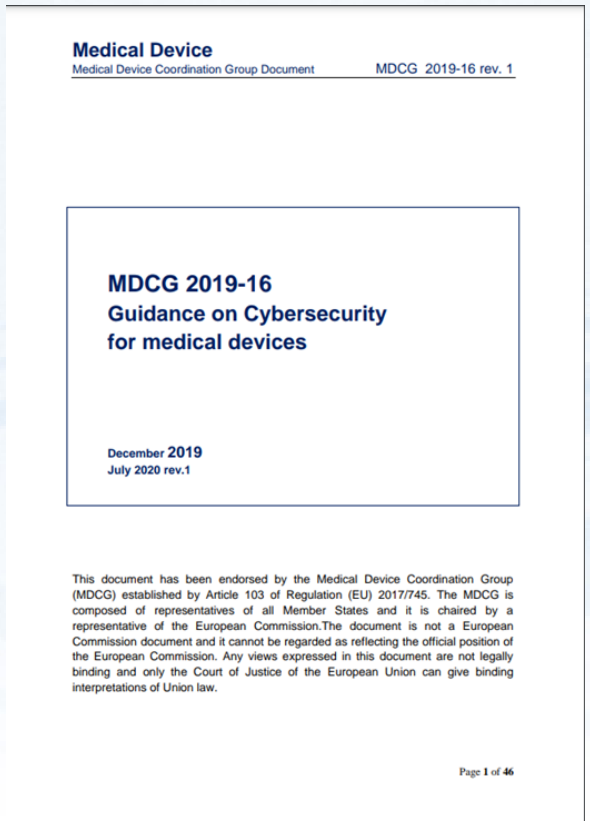
Status for norsk gjennomføring

De nye forordningene er tatt inn i EØS-avtalen vedlegg II, kapittel XXX om medisinsk utstyr. Det vil være behov for tilpasningstekster til EØS-komitebeslutningen som foreløpig er vurdert å være av teknisk/institusjonell art.

Helse- og omsorgsdepartementet har gjennomført høring om forslag til ny lov og forskrift om medisinsk utstyr. Departementet har fremmet forslag til ny lov om medisinsk utstyr for Stortinget. Stortinget samtykket 17. april 2020 til at EUs forordninger om medisinsk utstyr ble innlemmet i EØS-avtalen og tas inn i norsk rett. Loven vil tre i kraft samtidig som i EU-landene, 26 mai 2021.

https://legemiddelverket.no/medisinsk-utstyr/nye-forordninger-for-medisinsk-utstyr#status-for-norsk-gjennomf%C3%B8ring

MDCG 2019-16 Guidance on Cybersecurity for medical devices



Medical Device
Medical Device Coordination Group Document MDCG 2019-16 rev. 1

MDCG 2019-16
Guidance on Cybersecurity
for medical devices

December 2019
July 2020 rev.1

This document has been endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission.The document is not a European Commission document and it cannot be regarded as reflecting the official position of the European Commission. Any views expressed in this document are not legally binding and only the Court of Justice of the European Union can give binding interpretations of Union law.

Page 1 of 46

MDCG:Medical Device Coordination Group

St. Olavs driftsservice

ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

MDCG 2019-16 Guidance on Cybersecurity for medical devices

3.8. Lifecycle Aspects

Addressing cybersecurity risks at the design stage can help mitigate cybersecurity risks that could contribute to a breach in the confidentiality, a compromise in the integrity and availability of the medical device and its data, or intentional unauthorised access to the medical device and/or the network. Compromised CIA might impact medical purposes as specified in the medical device definition in MDR Article 2.

Other than for safety related hazards, whose number is quite stable over time, the security situation for software may change rapidly due to newly emerging security vulnerabilities, or due to new attack vectors.

This may lead to the situation that a medical device is considered secure with respect to known vulnerabilities at a specific point in time. However, ithout any security maintenance that device may become unsecure and possibly unsafe as a consequence due to newly emerging vulnerabilities or due to novel attack methods. During the support lifetime of the device, the manufacturer should put in place a process to gather post-market information with respect to the security of the device (see also Chapter 6). This process should take into account:

1. Security incidents directly related to medical device software
2. Security Vulnerabilities that are related to the medical device hardware/software and the 3rd party hardware/software used with the medical device.
3. Changes in the threat landscape, including interoperability aspects

The manufacturer should evaluate the information thus gathered, evaluate the associated security and safety risk and take appropriate measures that control the risk associated with such security incidents or vulnerabilities.

Measures may include:

- Information to operators of medical devices on the identified risk and possible mitigations in the operating environment
- Quick fixes, e.g. network configuration changes
- Medical device software updates
- **3rd party software updates or patches**. The measures should be implemented at the operator site in a time appropriate to the security and safety risk determined by the manufacturer and operator.

St. Olavs driftsservice

ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

https://ec.europa.eu/docsroom/documents/38941/attachments/1/translations/en/renditions/native

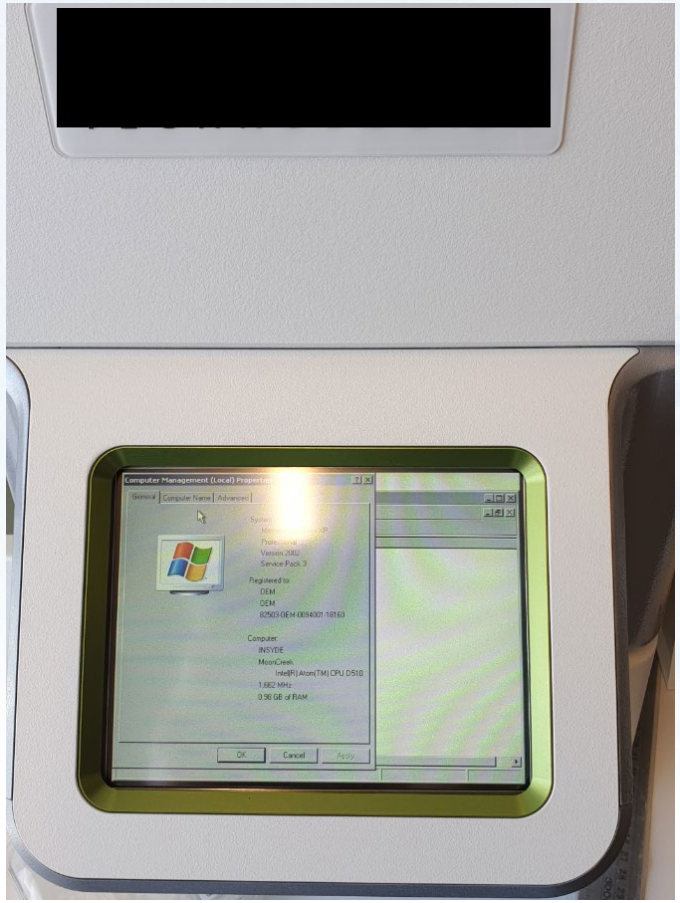
2.6. Joint Responsibility - Specific expectations from other stakeholders…

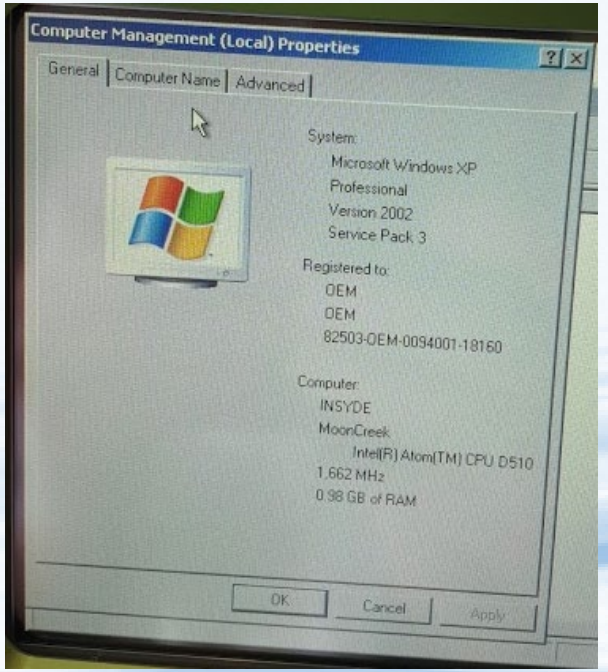
Modification of a medical device, e.g. the installation or enabling of third-party software including software patching, should always be under explicit published guidance of the manufacturer. It is important to understand that any invalidated modification of a medical device or system (e.g., product firewall changes, software patches, security software, utilities, games, music files, other software programs, etc.) can adversely affect system performance or safety in unpredictable ways. For example, it may open doors for easy exploitation of identified vulnerabilities of the medical device.

Vi er avhengig av at produsent tillatter / støtter patching – dette blir vektlagt I anskaffelser.

https://ec.europa.eu/health/sites/health/files/md_sector/docs/md_cybersecurity_en.pdf

Nytt utstyr installert på St. Olav 25. februar 2020





St. Olavs driftsservice

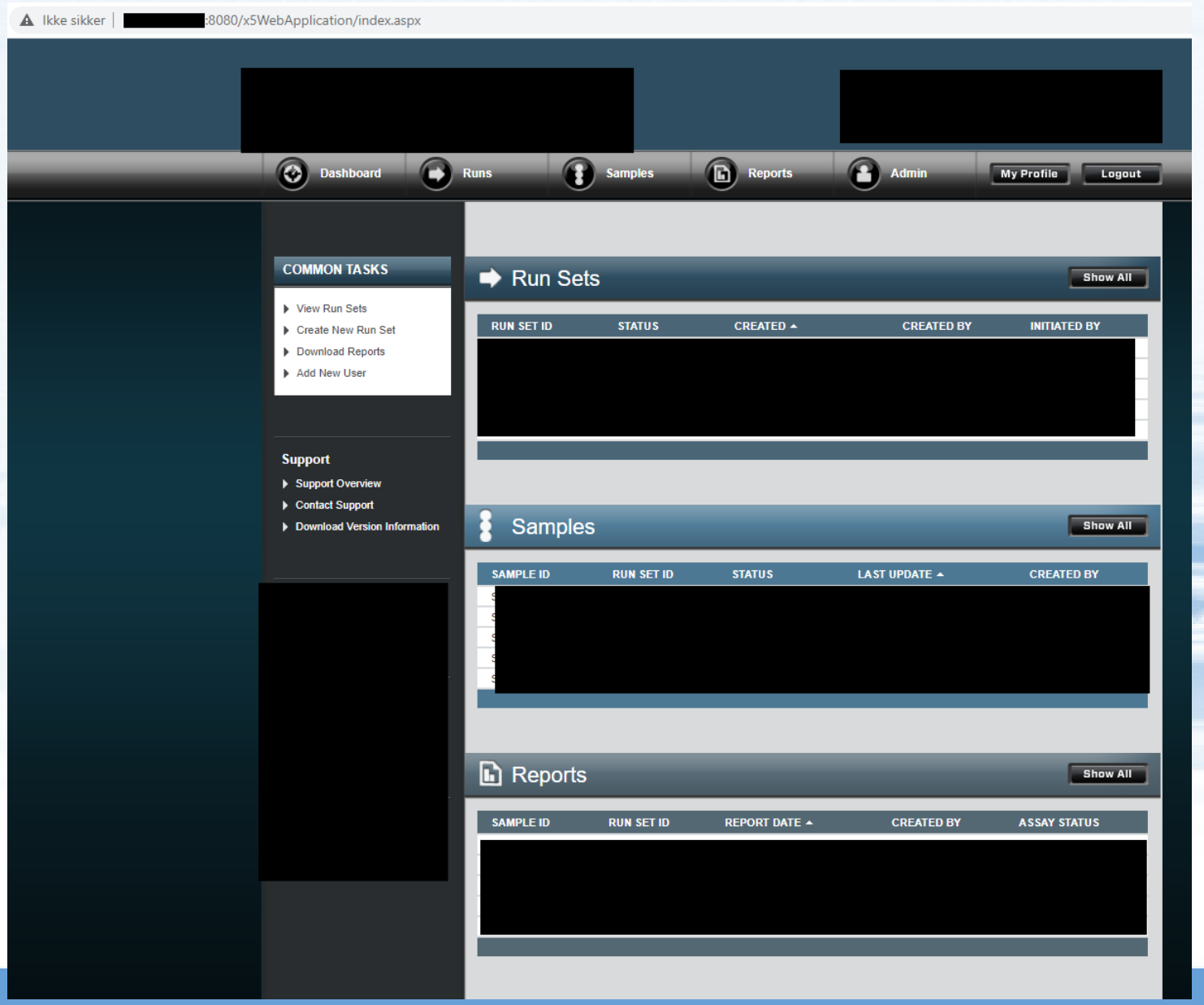
ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

Kundestøtte for Windows XP avviklet

Etter 12 år ble kundestøtte for Windows XP avviklet 8. april 2014. Microsoft vil ikke lenger tilby sikkerhetsoppdateringer eller teknisk støtte for operativsystemet Windows XP. Det er kritisk å overføre nå til et moderne operativsystem. Den beste måten å overføre fra Windows XP til Windows 10 på er å kjøpe en ny enhet.

Hvordan man får ut rapportene

Webside som man laster ned pdf



St. Olavs driftsservice

En pågående sak

Hei,

Vår [redacted] for stroboskopi på Nevrosenteret holder på å få full disk.

Jeg skal ordne nettverkstilgang (Så det sto et nettverkskort i) og få opprettet et filshare hvor de kan lagre pasientdata.

Trenger jeg en spesiell systembruker på Windows-maskinen for å få rettigheter til å legge det opp?

Er det noe spesielt jeg må tenke på i programvaren for å knytte opp sharet når jeg har mappet det opp?

Svar fra leverandøren

Er usikker på om du kan knytte systemet til fileshare.

Tror ikke det skal være et problem å få rettigheter på maskinen. Tror systembrukeren er administrator.

Forhører meg med [redacted] om det finnes en service bruker og om det går an å endre lagringslokasjonen.
Det som er at SW til denne maskinen er knyttet opp til de fysiske diskene og lagrer automatisk all data der. Når diskene er fulle må de byttes ut.
Du kan selvfølgelig flytte undersøkelsene manuelt, men da vil du miste fordelen ved at databasen vet hvilken disk undersøkelsene ligger på. Så hvis man skal se en spesifikk undersøkelse vil databasen fortelle hvilken disk man skal sette inn.

Det e sikkert noe gammelt utstyr…

Levert 12.01.2017

Og hva med en disk på avvei eller en disk som er blitt ødelagt? Beskyttelse? Tilgjengeligheten?

…men jeg leverer jo bare et lite MTU-system og et dataprogram som lagrer undersøkelsene…

<u>Og plutselig har vi et behandlingsrettet helseregister.</u>

- Som krever at data er korrekt og lagret på rett pasient – da bør det på plass en integrasjon for å hente pasientlister / spørringer.
- Det bør blir tilgjengeliggjort i pasientens hovedjournal – integrasjon
- Vi bør sikre at kun de som skal ha tilgang til systemet får tilgang – da bør det integreres mot IAM

- https://lovdata.no/lov/2014-06-20-43/§2
- https://lovdata.no/lov/2014-06-20-42/§2

St. Olavs driftsservice

ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

GDPR og informasjonssikkerhet

Det handler ikke bare om beskyttelse, det handler også om tilgjengelighet

St. Olavs driftsservice

ST. OLAVS HOSPITAL
UNIVERSITETSSYKEHUSET I TRONDHEIM

Foto: **Helle Merete Næss**

Status fra Normen om medisinsk utstyr og informasjonssikkerhet

Jan Gunnar Broch, Direktoratet for e-helse/ Sekretariatet for Normen

Webinar 7.april 2021

Et ferskt eksempel

Sektoren har noen særlige utfordringer

- Sikkerhetshendelser kan påvirke både pasientsikkerhet og personvern

- Fragmentert og komplekst aktørbilde – men sektoren utgjør en samlet eksponeringsflate inn mot felles verdier

NORMEN

MDR 26.5.2020 og IVDR 26.5.2022
- betydning for cybersikkerhet

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.**

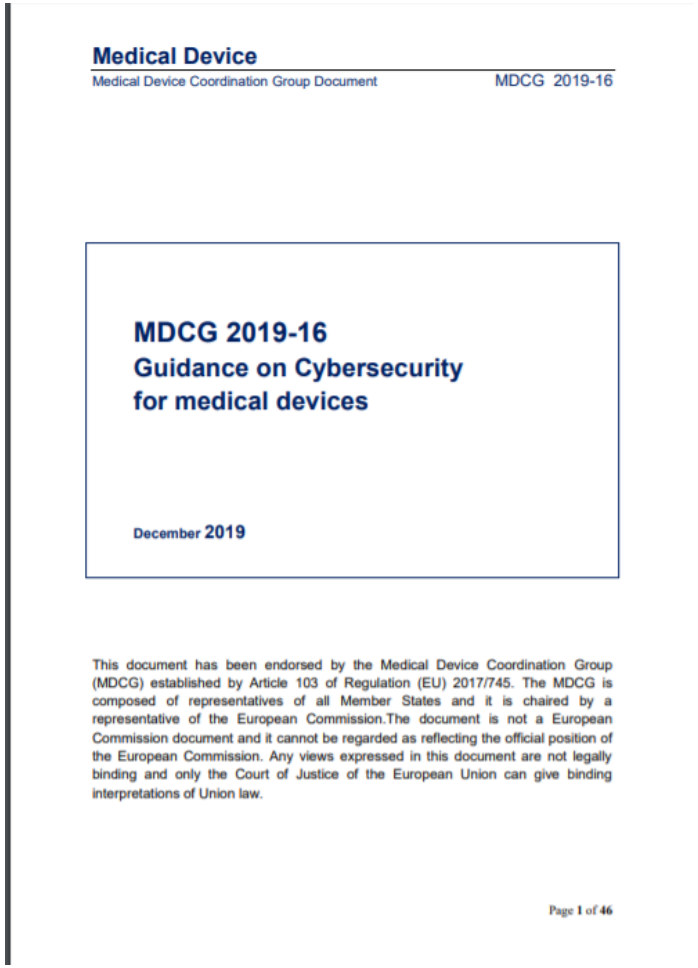
- 17.2. For devices that incorporate software or for software that are devices in themselves, **the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security,** verification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

MDCG 2019 -16
Guidance on Cybersecurity for medical devices

- Introduction
- Basic cybersecurity concepts
- Secure Design and Manufacture
- Documentation and Instructions for use
- Post-Market Surveillance and Vigilance
- Other Legislation and guidance: EU and international



Medical Device

Medical Device Coordination Group Document MDCG 2019-16

MDCG 2019-16
Guidance on Cybersecurity
for medical devices

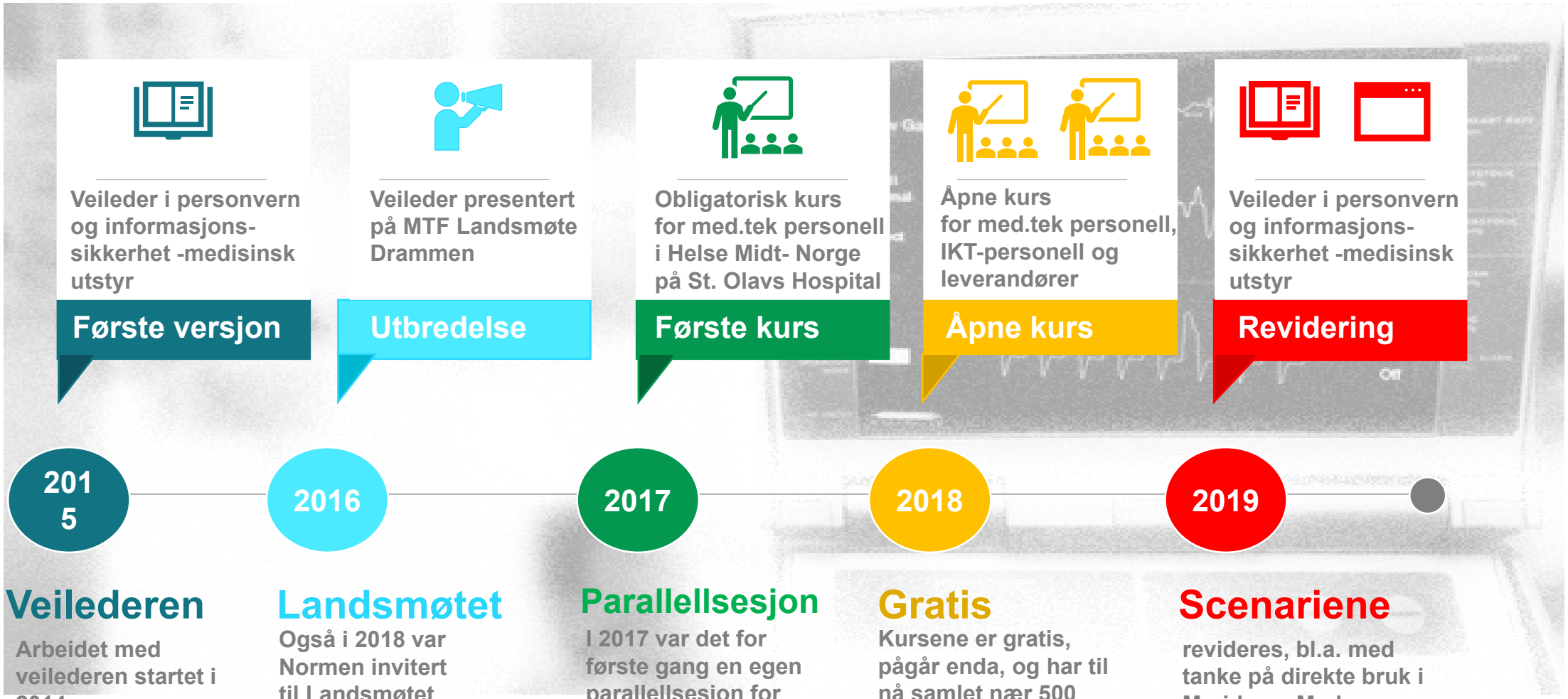
December 2019

This document has been endorsed by the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. The MDCG is composed of representatives of all Member States and it is chaired by a representative of the European Commission.The document is not a European Commission document and it cannot be regarded as reflecting the official position of the European Commission. Any views expressed in this document are not legally binding and only the Court of Justice of the European Union can give binding interpretations of Union law.

Page 1 of 46

NORMEN

Normen og medisinsk utstyr



2015

Veilederen

Arbeidet med veilederen startet i 2014

Første versjon

Veileder i personvern og informasjons-sikkerhet -medisinsk utstyr

2016

Landsmøtet

Også i 2018 var Normen invitert til Landsmøtet

Utbredelse

Veileder presentert på MTF Landsmøte Drammen

2017

Parallellsesjon

I 2017 var det for første gang en egen parallellsesjon for medisinsk utstyr og informasjonssikkerhet på Normkonferansen

Første kurs

Obligatorisk kurs for med.tek personell i Helse Midt- Norge på St. Olavs Hospital

2018

Gratis

Kursene er gratis, pågår enda, og har til nå samlet nær 500 deltakere

Åpne kurs

Åpne kurs for med.tek personell, IKT-personell og leverandører

2019

Scenariene

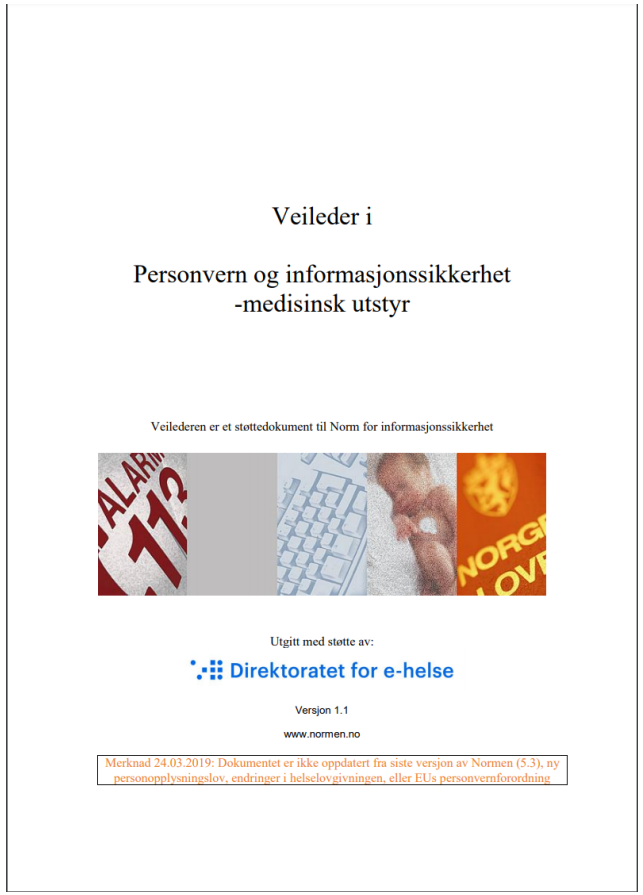
revideres, bl.a. med tanke på direkte bruk i Merida og Medusa

Revidering

Veileder i personvern og informasjons-sikkerhet -medisinsk utstyr

NORMEN

Revidering av Normens veileder medisinsk utstyr


Veileder i

Personvern og informasjonssikkerhet
-medisinsk utstyr

Veilederen er et støttedokument til Norm for informasjonssikkerhet

Utgitt med støtte av:

Direktoratet for e-helse

Versjon 1.1

www.normen.no

Merknad 24.03.2019: Dokumentet er ikke oppdatert fra siste versjon av Normen (5.3), ny personopplysningslov, endringer i helselovgivningen, eller EUs personvernforordning

- Revidert struktur
  - Nye bruksscenarier
- Oppdatert etter ny personopplysningslov (GDPR)
- Oppdatert omtale av trusler og tiltak
  - Ser på MDCG 2019-16

NORMEN

Flere spørsmål?

www.normen.no
sikkerhetsnormen@ehelse.no