Direktoratet for e-helse

INFORMASJONSSIKKERHET

Jan Gunnar Broch, Direktoratet for e-helse
Akkrediteringsdag for medisinske laboratorier
7.12.2017

DIREKTORATET FOR E-HELSE

Myndighet

Sørge for nasjonal styring og koordinering

Nasjonale e-helseløsninger

Få på plass og forvalte digitale løsninger som forbedrer og forenkler


Informasjonssikkerhet – hva er det?
NORMEN
Informasjonssikkerhet og medisinsk utstyr
Direktoratet for e-helse
Side 3


Informasjonssikkerhet – hva er det?
Direktoratet for e-helse
Side 4

Informasjonssikkerhet/ IT-sikkerhet
Helse - K I T

- Tilgjengelighet
- Integritet
- Konfidensialitet

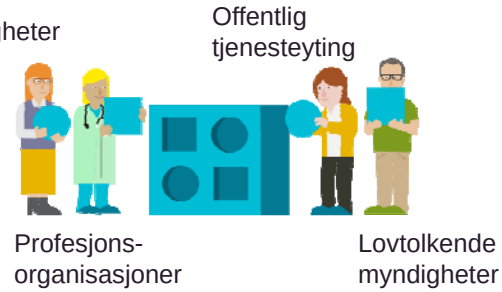
«Hva er det verste som kan skje?
Det kan skje verre ting med journalen din enn at at uvedkommende får innsyn i den. Det mener kronikkforfatteren, som til daglig arbeider i Nasjonal sikkerhetsmyndighet.»

Roar Thon, Fagbladet Journalen

NORMEN

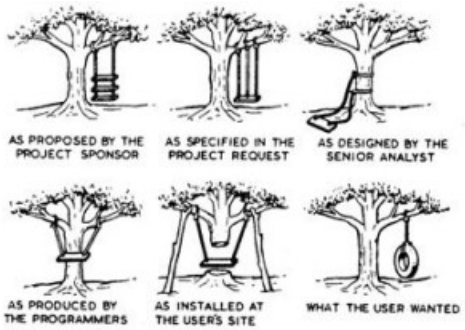
Norm for informasjonssikkerhet i helse- og omsorgssektoren

- Bransjenorm – samler krav fra flere lover og forskrifter i et dokument
- Utviklet og vedlikeholdes av styringsgruppe fra sektoren
- Sekretariat fra Direktoratet for e-helse og Norsk Helsenett
- Referansegrupper med deltakere fra sektoren og utenfor som har relevant input



Om krav i Normen

- Er minimumskrav
  - Fritar selvsagt ikke for risikovurdering
  - Bruk av andre «beste praksis» kan være nødvendig
    - **ISO 15189:2012**
- Normen er teknologinøytral
- «Tekniske krav» stort sett uendret fra 2006
  - Utdypet i nyere faktaark og veiledere
- Normens krav dekker alle
  - Fra fotpleieren på hjørnet til nasjonale løsninger
  - Hvordan skalerer kravene?



Normen og GDPR

25. mai 2018

Personopplysnings-forskriften oppheves

Artikkel 32 – Sikkerhet ved behandlingen

Idet det tas hensyn til det tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt [illegible] og [illegible] som er [illegible] etter

«Overholdelse av godkjente **atferdsnormer** som nevnt i artikkel 40 eller en godkjent sertifiseringsmekanisme som nevnt i artikkel 42 kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt»

Norm for informasjonssikkerhet
Bindende gjennom tilknytningsavtale med NHN

- Styrende del
- Gjennomførende del
- Kontrollerende del

Veiledere
Faktaark

Ikke bindende

Normen (”Code of conduct”) og en del faktaark / veiledere er oversatt til engelsk

Eksempler – veiledere og

- Veileder for informasjonssikke
  personvern – medisinsk utsty
- Veileder for legekontor
- Veileder for sosiale media
- Veileder for skytjenester
- Faktaark 6b - Sikkerhetsrevisj
- Faktaark 10 - Bruk av databeh
- Faktaark 29 - Hjemmekontor
- Faktaark 38 - Sikkerhetskrav t

39	Elektronisk utlevering til kontrollkommisjon	2.1	12/09
40	Informasjonssikkerhet i forskningsprosjekter	1.1	06/09
41	Skadereparasjon når data har blitt utilsiktet utlevert	2.1	12/09
42	Bruk av SMS i pasientkontakt	1.1	06/09
43	Bruk av testdata i systemer som inneholder helse- og personopplysninger	1.1	06/09
44	Personvern og informasjonssikkerhet i helse- og sosialtjenesten - kortfattet oversikt for kommuneledelsen	1.1	06/09
45	Personvern og informasjonssikkerhet - en kort orientering for det enkelte helse- og sosialpersonell i kommuner	1.1	06/09
46	Databehandlingsansvar og avtaler i forbindelse med tjenesteutsetting	2.0	06/11
47	Autorisasjonsregister	1.1	06/10
48	Informasjonssikkerhet ved utførelse av testing	1.1	01/10
49	Krav ved bruk av PKI ved ekstern kommunikasjon	1.1	06/10
50	Innsyn i hendelsesregistre	1.1	06/10
51	Innsyn i den ansattes e-postkasse mv	1.1	10/10
52	Krav til teknisk løsning ved bruk av betalingsterminal	1.0	06/11

Direktoratet for e-helse

Andre aktiviteter i regi av Normen

Normkonferansen 2017

November 2017
Scandic Fornebu

Nyhetsbrev

- 4 ganger årlig
- Påmelding www.normen.no

Q&A epost

sikkerhetsnormen@ehelse.no

Kurs og foredrag

- Kurs
- Konferanser
- Foredrag

www.normen.no

- Alle dokumentene
- Nyheter
- Om Normen

Sosiale medier

Normen på FB

@Normen_no

Direktoratet for e-helse

Informasjonssikkerhet og medisinsk utstyr

Før:

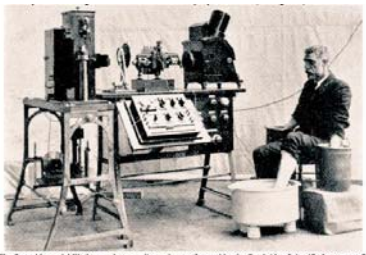


Fig. 6. The first table-model Einthoven electrocardiograph manufactured by the Cambridge Scientific Instrument Company of London in 1911. On the right hand side the arch lamp, in the centre on the table the string galvanometer, and below the switching board for the leads, next left to the camera the 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:

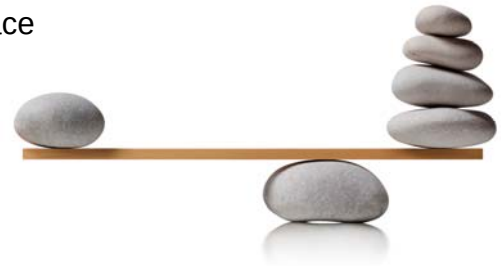
- «Alt» er tilkoblet nettverk
- Måleresultater og innstillinger overføres til sentrale servere/applikasjoner
- Muligheter for brukertilpasset menyer, alarmer, bilder osv.
- Sikkerhetsfunksjoner for å unngå feilbehandling.

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



«GE-saken»

DAGENS Medisin

Leder: Vi skal være glade for prioriterings-dilemmaene

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

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
2009
2008
2007

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)

1 Innledning

Personvernnemnda har ved oversendelse fra Datatilsynet mottatt klage på Datatilsynets vedtak om pålegg vedrørende uautorisert uthenting av helseopplysninger gjennom leverandørs fjerntilgang.

Aftenposten A-magasinet Osloby Sport Meninger Jan Gunnar | Meny

Osloby Restaurantguiden Sulten Byliv

Pasientopplysninger fra flere Oslo-sykehus på avveie i over fem år

ERLEND TRO KLETTE

OPPDATERT: 10.APR.2017 13:46 | PUBLISERT: 10.APR.2017 13:45

Sensitive personopplysninger om mer enn 10 000 pasienter ved tre Oslo-sykehus ble lagret på amerikanske servere i over fem år før de ble slettet, ifølge Vårt Oslo. Sykehusene visste ingenting om sikkerhetssvikten.

Riksrevisjonens selskapskontroll 2014

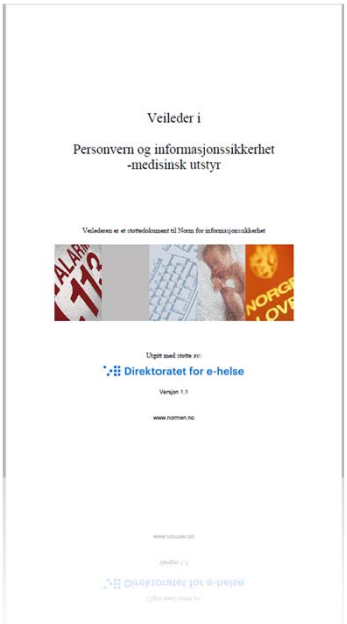
Sak 3: Helseforetakenes ivaretakelse av informasjonssikkerhet i medisinsk-teknisk utstyr

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.

Normens arbeid med informasjonssikkerhet og medisinsk utstyr

- Utviklet egen veileder for informasjonssikkerhet og medisinsk utstyr i 2015
- Kurs basert på Normens veileder i alle regioner i 2017
  - Samarbeid med med.tek avdelinger, Normsekretariatet og HelseCERT
  - Nytt kurs 2018
- Flere regioner arbeider med risikovurderinger av MTU, standardiserte kravsett og databehandleravtaler



Direktoratet for e-helse

Direktoratet for e-helse

Takk for meg!

jan.gunnar.broch@ehelse.no

Normen

www.normen.no/ www.ehelse.no