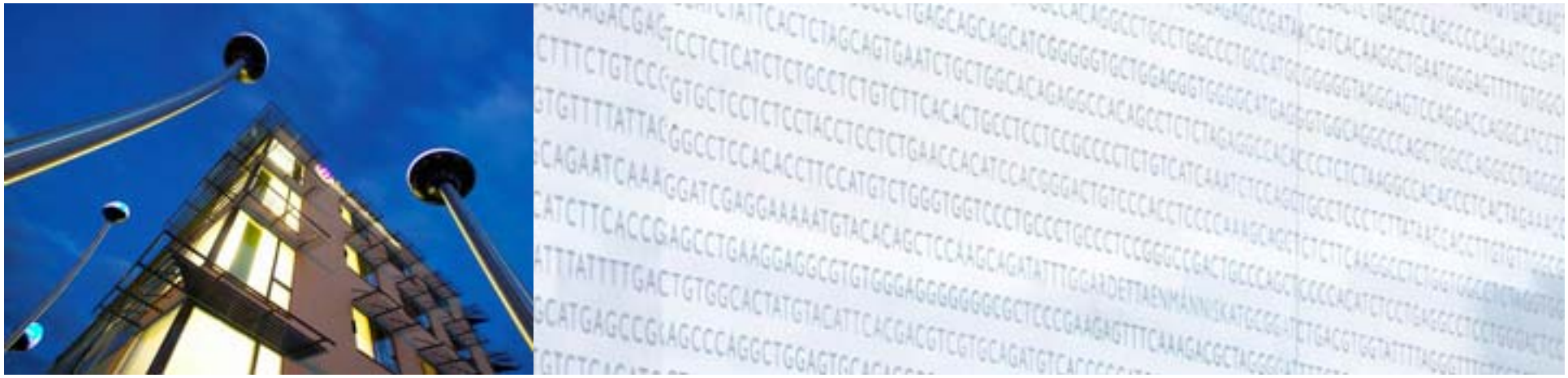


Informationssäkerhet och medicintekniska produkter

eller

Information security with respect to safety considerations

Mats Ohlson

LÄKEMEDELSVERKET
MEDICAL PRODUCTS AGENCY

Informationssäkerhet = Information security

- **Informationssäkerhet**
  - the preservation of confidentiality, integrity and availability of information
    - ISO/IEC 27000_2014.
  - “bevarande av informationens konfidentialitet, riktighet och tillgänglighet”

Eventuell målkonflikt

- **Problemet:**
  - felaktig hantering eller överföring av information med en medicinsk programvara kan leda till felaktig eller fördröjd diagnos eller behandling
  - IMDRF
    - Factors relating to information security may affect the integrity, availability, or accessibility of information output from the SaMD needed for correct diagnosis or treatment
      - Guideline N12 SaMD software as medical devices
      - International Medical Device Regulators Forum

Försvårande faktorer

- Begränsningar i användaråtkomst
  - SaMD används vanligen av flera olika användare med olika behov eller begränsningar av åtkomst med hänsyn till informationssäkerhetsregler
- Gemensamma plattformar
  - Plattformar där SaMD är installerade delas ofta med andra programvaruappligationer.
- Externa kopplingar
  - SaMD är ofta kopplade till Internet, nätverk, databaser eller servrar med varierande informationssäkerhetskrav.

IMDRF:
Att tänka på för ansvarig tillverkare utifrån krav på informationssäkerhet:

- **Balansera behoven**
  - att krav på säkerhet och konfidentialitet balanseras med kliniska/medicinska behov av tillgänglighet.

- **Kommunikation av data**
  - att identifiera, realisera och införa säkra (och formaliserade) sätt att lagra, omvandla och/eller överföra data.

Tillverkaren ska ta hänsyn till

- **Behovet av samtidig access**
  - att konstruktionen med tanke på datasäkerhet tillämpar lämpliga styr- och kontrollmetoder när informationen ska nås av flera applikationer och användare.
- **Säkert införande av uppdateringar**
  - att det ska vara praktiskt möjligt för användaren att införa säkerhetsuppdateringar.
- **Åtkomstkontroll**
  - att det finns möjlighet till adekvat åtkomstkontroll och begränsningar för
    - skydd av känslig information
    - systeminställningar och platser med viktig information.

Tänk också på …

- **Eventuell skadlig interaktion mellan system**
  - Konstruktionen med hänsyn till eventuell skadlig interaktion mellan olika system
  - Lämpliga funktioner för återhämtning och robusthet.

- **Användarinformationen. Hur man på ett säkert sätt:**
  - Installerar SaMD i lämplig programvarumiljö (t ex. OS, integration med annan programvara);
  - Hanterar autentiseringsverktygen
  - Uppdaterar virusskydd, operativsystem, andra system och tillämpningar

Vem ska ta ansvar för vad?

Informationssäkerhet

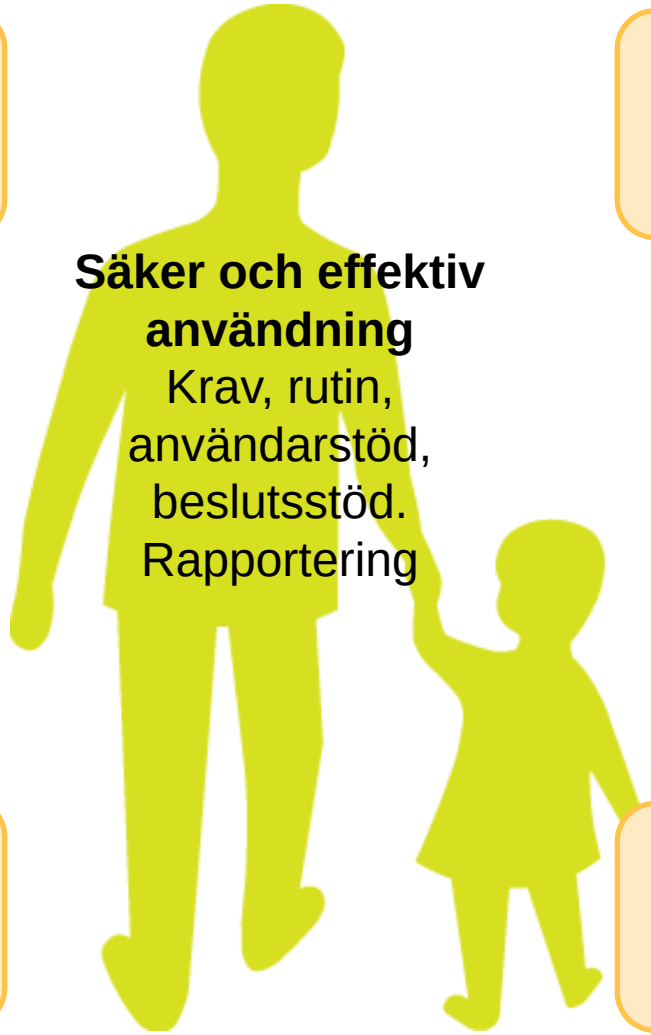
Ett samarbete med patienter i centrum

Upphandling
Kundkrav
Beställarens krav

Metoder
Vetenskap
Algoritmer
(Terminologi)

Standarder
Strukturer
Gränssnitt
Terminologi

Produkter
Säkra produkter
Utvärdering



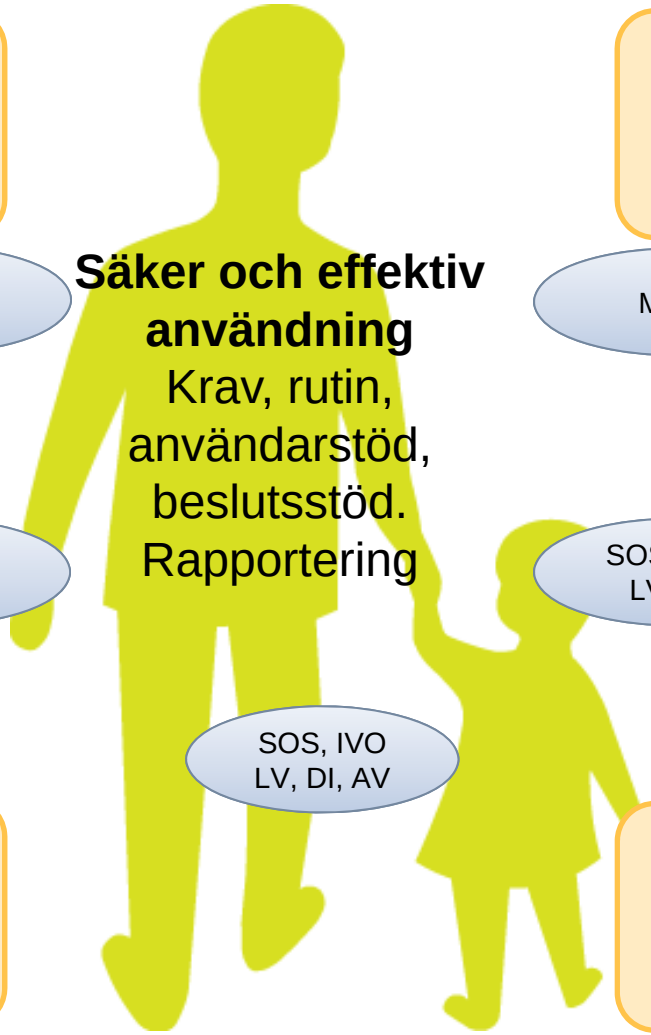
Programvaror
Bearbetar data
Presenterar data

Infrastruktur
Mjuk infrastruktur
Hård infrastruktur
Kommunikation

Information /data
Nationella databaser
Regionala databaser
Info hos vårdgivare

Förvaltning
Uppdateringar
Backup, SW / HW
Sköta databaser

Tillsynsbilden är inte komplett



Konkurrens verket, IVO

Upphandling
Kundkrav
Beställarens krav

LV (DI, AV)

Programvaror
Bearbetar data
Presenterar data

Metoder
Vetenskap
Algoritmer
(Terminologi)

SOS, LV

Säker och effektiv användning
Krav, rutin, användarstöd, beslutsstöd.
Rapportering

MSB

Infrastruktur
Mjuk infrastruktur
Hård infrastruktur
Kommunikation

Standarder
Strukturer
Gränssnitt
Terminologi

SOS, LV

SOS, IVO
LV, DI

Information /data
Nationella databaser
Regionala databaser
Info hos vårdgivare

SOS, IVO
LV, DI, AV

LV, TLV

Produkter
Säkra produkter
Utvärdering

SOS, IVO
DI

Förvaltning
Uppdateringar
Backup, SW / HW
Sköta databaser

Vem förväntas göra vad?

- **Regler för informationssäkerhet riktar sig till olika aktörer:**
  - Rena säkerhetskrav (riktighet, tillgänglighet) till tillverkare
  - Sekretesskrav till användarna

- **Viss medvetenhet om problemet börjar synas …**