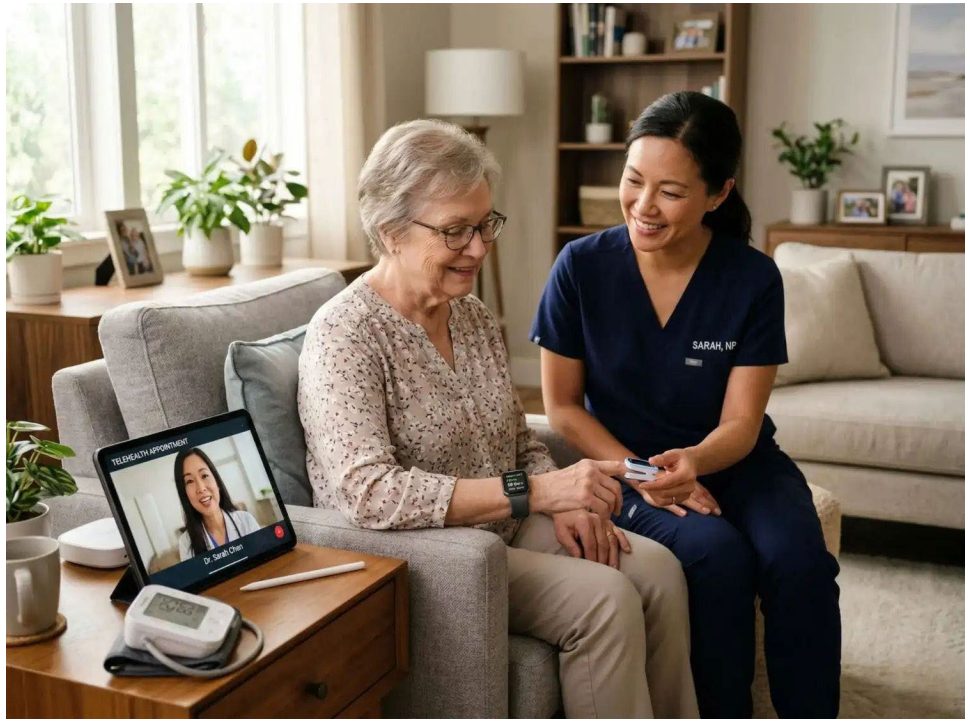
Nordic Cyber for Healthcare Forum

by DNV

Scaling Hospital@Home, a Nordic approach to medical device security



Ambition: make it faster and safer to adopt medical devices in patients' homes.

Nordic Cyber for Healthcare Forum

A unique, invitation-only network for leaders in risk management and cybersecurity across the Nordic healthcare sector, to strengthen preparedness against common cyber threats.

A multidisciplinary approach that brings together security experts, clinicians, and senior leadership..

Strong connections to international networks and initiatives within healthcare cybersecurity.

Promote a proactive approach to new EU regulations.

Move from networking to concrete Nordic collaboration through joint initiatives and exercises.

DNV
CYBER

Ambitions

Strengthen the cyber preparedness of the Nordic healthcare ecosystem— by ensuring an open, actionable exchange of knowledge, experience and best practices.

Unique, cross disciplinary platform, extending from information sharing to practical collaboration

DNV
CYBER

TIMELINE

Inaugeration meeting
DNV HQ
August 29 2024
11 participants.

2. meeting
Rigshospitalet
November 26 2024
21 participants

3. meeting
Karolinska University Hospital
May 8-9 2025
35 participants

4. meeting
Helsinki University Hospital
12.-13. November 2025
39 participants

5. meeting
Oslo University Hospital and Sykehuspartner
19.-20. March 2026
50 participants

6. meeting:
CEPT Brussel and University hospitals Leuven, 21.-22. oktober
50 participants

Medical device security working group

DNV CYBER

Participants & Contributor Ecosystem

Nordic Cyber for Healthcare Forum brings together a unique cross-disciplinary group.

Core Nordic participants

Who we have in the room

National health authorities

Policy level and regulators, including health directorates and agencies. agencies.

University hospitals and health regions

Leading Nordic providers with operational experience and implementation responsibility.

Security, emergency preparedness and resilience leaders

Cybersecurity, risk management and crisis-preparedness functions.

Clinicians and senior leadership

Clinical experts and executives who can translate strategy into practical change practical change

International contributors

Relevant networks and institutions we involve

European Commission
DG Connect

EU Agency for Cybersecurity
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

WHO
World Health Organization
European Region

Hybrid CoE
Centre of Excellence Countering Hybrid Threats

Health-ISAC™
Collaborating for Resilience in Healthcare
Healthcare cybersecurity sharing network

Combines authority-level, clinical leadership and cyber expertise to accelerate Nordic healthcare resilience.

DNV
CYBER

Nordic Cyber for Healthcare Forum by DNV

Medical Device Security Working Group

Hospital@Home: From individual pilots to secure, reusable Nordic scaling

1 Shared challenge

An ageing population, workforce shortages and growing pressure on hospital capacity.

2 Shared barrier

Security, privacy and regulatory assessments are repeated across organisations.

3 Shared solution

A Nordic library of methods, documentation and security requirements.

NO — SE — DK — FI — IS

Ambition: make it faster and safer to adopt clinically relevant medical devices in patients' homes.

Medical Device Security Working Group

Medical Device Security Working Group

01 Part of the Nordic Cyber for Healthcare Forum

02 Monthly working sessions

03 Approximately 25 participants across Nordic countries

DNV

CYBER

Hospital@Home and Remote Patient Monitoring

Can we realize security benefits and improve patient care, with reduced local costs, time and resources?

Unique Nordic collaboration

The project brings together healthcare stakeholders to address a shared need across the region.

Common needs across five countries

Combines health policy priorities with clinical, cybersecurity and regulatory requirements across all Nordic countries.

Political and authority-level dialogue

Ongoing dialogue with the Nordic Council of Ministers, with orientation to national health authorities.

Why this matters

A focused project to convert Nordic alignment into reusable methods, documentation and security requirements that can support safer and more cost-effective deployment of digital care at home.

DNV
CYBER

CURRENT STATE:

Security & Compliance Slow the Scale-Up of Remote Patient Monitoring

Challenge:As Hospital@Home and Remote Patient Monitoring (RPM) expands to support chronic disease management, each hospital, region, and project team must independently perform security, privacy, and compliance activities before solutions can be deployed.

CURRENT WORKFLOW (TODAY)

1. Clinical Need Identified
2. Select RPM Vendor / Solution
3. Local Security Reviews
4. Risk Assessments with Increasing Complexity
5. Compliance & Procurement Review
6. Approval for Pilot / Deployment

TODAY'S PAIN POINTS

TIME-CONSUMING RISK ASSESSMENTS

- Each hospital repeats similar assessments
- Limited reuse of vendor evidence and results

INCONSISTENT REQUIREMENTS

- Different criteria and templates by region
- Limited reuse of evidence and documentation
- Security baselines are not aligned

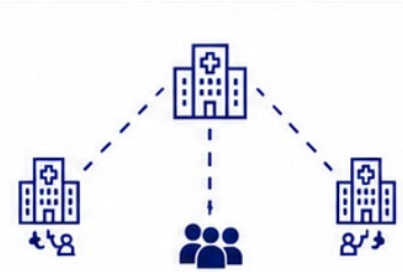
SLOW ADOPTION

- Security reviews become a bottleneck
- Long approval cycles
- Deployment to patients is delayed

HIGHER COST

- Resources recreate assessments instead of improving care
- Operational and project costs increase

IMPACT



Security and compliance work is essential, but today clinical implementation is delayed even when the technology exists and the need is clear

PROPOSAL OF THE MEDICAL DEVICE SECURITY WORKING GROUP

- ✓ Reduce duplication
- Accelerate adoption
- Align across the Nordics
- ♥ Deliver better patient care

Proposal: a Nordic library for secure adoption at scale

“Assess once, reuse across the Nordics” applies to methods and documentation, not local decisions or approvals.

Standardised risk assessments

Selected patient groups and clinical use cases.

Shared security controls

A baseline for technical and organisational security.

Supplier checklists

Harmonised requirements based on MDS2 and expected evidence.

Regulatory documentation

Practical support for MDR, privacy and local compliance.

Outcome: faster, more consistent and safer implementation of Hospital@Home and remote patient monitoring services

DNV
CYBER

Proposed roles and responsibilities

SHARED NORDIC LEVEL

01 Develop methods and templates

02 Maintain a shared repository

03 Coordinate workshops and exchange experience

04 Document plans, progress and deliverables

LOCAL LEVEL

01 Decisions and governance

02 Accountability for local use

03 DPIAs, MDR/IVDR and local compliance

04 Clinical operations and risk acceptance

The library supports local decisions. Each organisation retains legal, clinical and regulatory accountability.

Implementation

Start focused, validate, then expand for reuse

01 Focus on clinical value

One or two Hospital@Home use cases, such as COPD or heart failure.

02 Nordic team

A cross-functional team from 4 countries ready

03 Validation and expansion

Test the model in Nordic hospitals, measure its impact and extend it to additional use cases.

DNV CYBER

In the next phase, we welcome collaboration across Europe

Relevance to European healthcare

- Similar patient groups
- The same security challenges
- The same regulatory requirements
- The same vendors

Opportunity to expand further

Build on Nordic collaboration initiated with clear relevance to

- Health preparedness,
- Cybersecurity and
- Digital transformation.

Expected impact

- Less duplicated work
- Faster procurement
- Stronger security
- Safer clinical implementation
- Lower cost

Thank you for your attention!

Morten Thorkildsen

Project Lead, Nordic Cyber for Healthcare Forum (DNV)

morten@morthork.com

DNV
CYBER