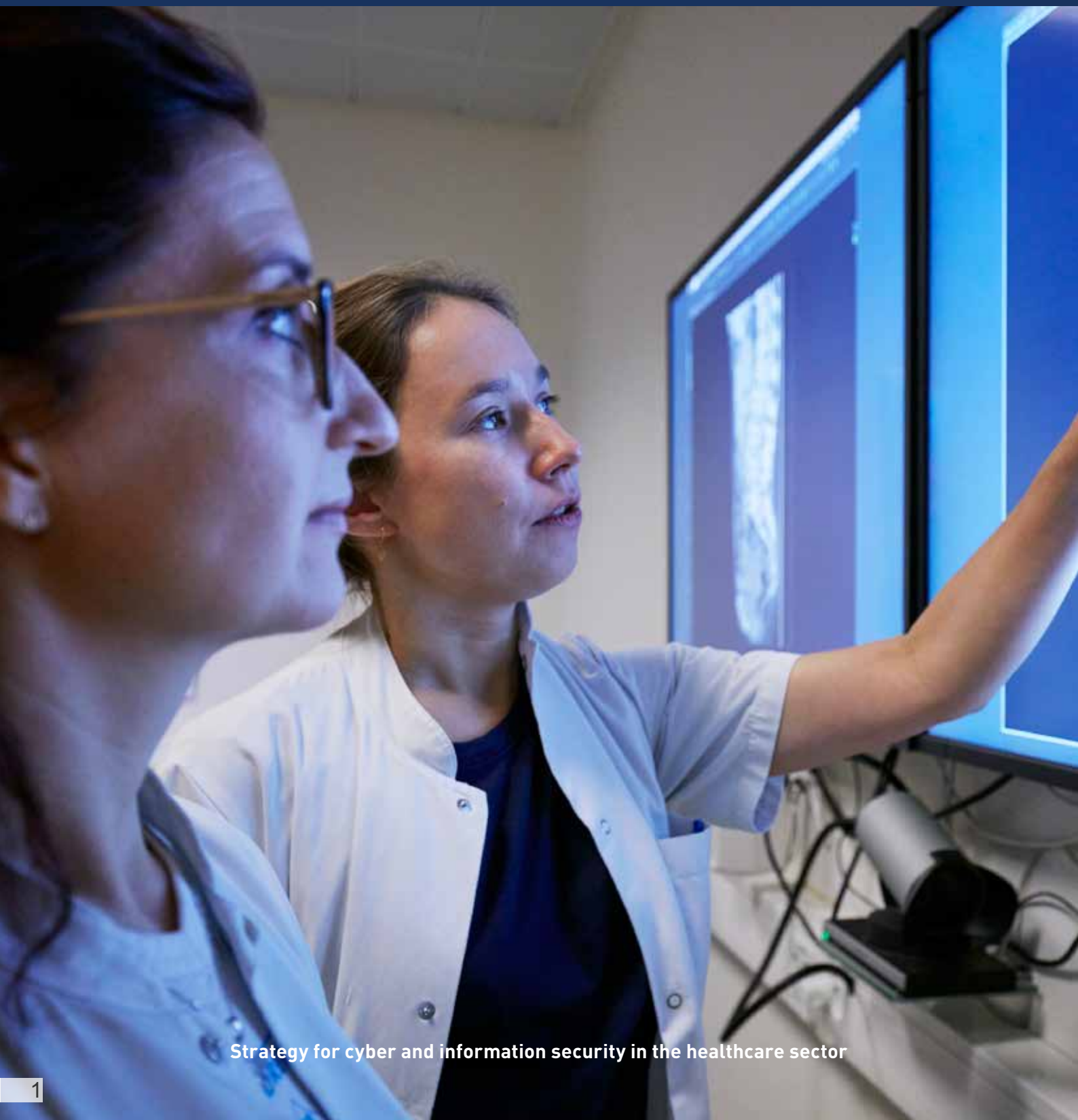


# A strengthened collective cyber and information security effort

---





# Contents

04	<b>PREFACE</b>	Increased peace of mind in a digitised healthcare system
06	<b>INTRODUCTION</b>	A strengthened collective effort
12	<b>WHERE ARE WE TODAY</b>	Everyone in our sector protects citizens and their health data
16	<b>BACKGROUND AND ANALYSIS</b>	Threats, vulnerabilities, and risks in the sector
22	<b>THE STRATEGIC MATRIX</b>	Four tracks to help us enhance cyber and information security
24	<b>TRACK 1 – PREDICT</b>	<b>Better prediction of potential attacks and incidents</b>
	1.1.	Identification of critical business processes and IT systems across actors within the sector
	1.2.	Better overview of the healthcare sector's vulnerabilities and risks
	1.3.	Effective coordination of notifications
	1.4.	Clear roles and responsibilities
	1.5.	Participation in relevant international forums on cyber and information security in healthcare
30	<b>TRACK 2 – PREVENT</b>	<b>Better prevention of attacks and incidents</b>
	2.1.	Security begins with the staff
	2.2.	Enhanced technical cyber and information security in the sector's systems and IT infrastructure
	2.3.	Managing security in legacy systems and equipment
	2.4.	Enhanced security in IoT devices
	2.5.	Increased security requirements for IT suppliers
	2.6.	Enhancing the sector's security architecture
38	<b>TRACK 3 – DETECT</b>	<b>Better detection of attacks and incidents</b>
	3.1.	Regular security tests in the healthcare sector's systems and equipment
	3.2.	Functions for monitoring and analysing activity in the healthcare sector's IT systems and infrastructure
	3.3.	Effective handling of suspicion of incidents
44	<b>TRACK 4 – RESPONSE</b>	<b>Rapid response in the event of attacks and incidents</b>
	4.1.	Incident response
	4.2.	Establishing cross-sectorial IT and cyber emergency response
	4.3.	Emergency response exercises for shared systems and supply chains
52	<b>FROM STRATEGY TO ACTION</b>	Implementation and continuous evaluation, prioritisation, and further development

# Increased peace of mind in a digitised healthcare service



Security has always been key in healthcare. The healthcare service exists to secure the lives and health of citizens. Treatment and care must take place under safe and secure conditions – this is a basic prerequisite. Hence security is already an integral part of everyday life in the Danish healthcare service.

As digital solutions become increasingly important within our healthcare service, safe and secure conditions also include strong cyber and information security. Digital tools will allow us to offer citizens and relatives a safe, accessible, and coherent healthcare service. A healthcare service where citizens can easily get in touch with their own general practitioner and hospitals, where all relevant information follows citizens along treatment pathways throughout the healthcare service, and where citizens can experience treatment and care in close proximity to their homes. There are many advantages. The Danish

**The Danish healthcare service is already one of the most digitised healthcare services in the world, and there is still great potential.**

healthcare service is already one of the most digitised healthcare services in the world, and there is still great potential.

However, with digitisation new challenges arise as well. As individuals and equipment at regional hospitals, in municipal care, at general practitioners, and among other healthcare providers become increasingly interconnected, the complexity of the systems increases and with it the healthcare service's vulnerability to cyber attacks. The threats take many forms and are constantly evolving. We take this challenge very seriously. The many ongoing cyber and information security efforts in various parts of the healthcare service provide a strong starting point from which to strengthen the sector as a whole.

The relationship between the healthcare service and the citizens rests on a foundation of trust. Trust in the

right diagnoses being made. Trust in citizens receiving the right treatment and care. And not least, trust in the healthcare service taking good care of the sensitive personal data that citizens hand over as part of their treatment. Maintaining citizen trust is crucial. Both citizens and healthcare professionals must still be able to trust that their data will be stored properly and securely, that relevant information can be accessed when necessary for treatment, and, not least, that data is correct so that patients can receive treatment on the right basis.

A coherent healthcare service also calls for increased coherence regarding cyber and information security. It is important that we all pull together as a whole. This is necessary to reap the benefits of digitisation. A con-

sistently high level of cyber and information security across the sector is a crucial element in our efforts to ensure that our healthcare service is future-proof.

With this strategy we aim to strengthen the joint and coordinated efforts further. We want to define a common agenda and the direction for the further cyber and information security efforts in the Danish healthcare service. We therefore embark together upon a common journey, but our ultimate goal is not defined by this strategy alone. This is a journey that will involve healthcare-sector actors working together throughout the strategy period to prioritise activities and agree on the funding of these. With this strategy we take the first collective steps.

#### **POLITICAL CYBER FORUM FOR THE HEALTHCARE SECTOR**

**Ellen Trane Nørby** Minister for Health

**Jette Skive** Chair of Local Government Denmark's  
Health and Elderly Committee

**Stephanie Lose** Chair of Danish Regions



# A strengthened collective effort

The healthcare sector is a critical sector in Denmark. Thousands of citizens come into contact with the healthcare service every day; and for many, the healthcare sector's ability to provide timely treatment and care is critical. Therefore it is important that the sector is able to ensure that the right treatment and care is available to citizens when needed.

Today, the Danish health sector is characterised by increasing digitisation. Every day large volumes of health data are handled digitally across many treatment units. The sector is working towards increasing cooperation regarding treatment and care with the assistance of digital exchange of information so that the way through the healthcare service is as safe and seamless as possible for citizens. As a result, dependency on digital infrastructure and data exchange is growing.

There are many advantages to digitisation. However, the many connected units and actors and the large volumes of sensitive personal data also make the healthcare sector vulnerable to cyber and information security incidents – such as potential cyber attacks. Hence it is necessary to enhance the sector's collective cyber and information security effort to secure the continued treatment and care of citizens and the protection of their sensitive personal data.

The healthcare sector is made up of many different healthcare providers that are organised and run in different ways; from large regional hospitals, offering highly specialised treatment, and municipal units for monitoring and care to smaller medical practices, clinics, and pharmacies. Most of these actors are publicly run, but many smaller actors – such as general practitioners, specialists, physiotherapists, dentists, etc. – are private business owners.

Moreover, the sector's portfolio of IT systems involves a distinct complexity that is managed in different ways; from huge IT system landscapes in the regions, with thousands of users and supported by some of Denmark's biggest IT departments, to small systems with few users in primary healthcare. In addition, there are challenges involving legacy systems and IoT devices with varying levels of security – which is also the case

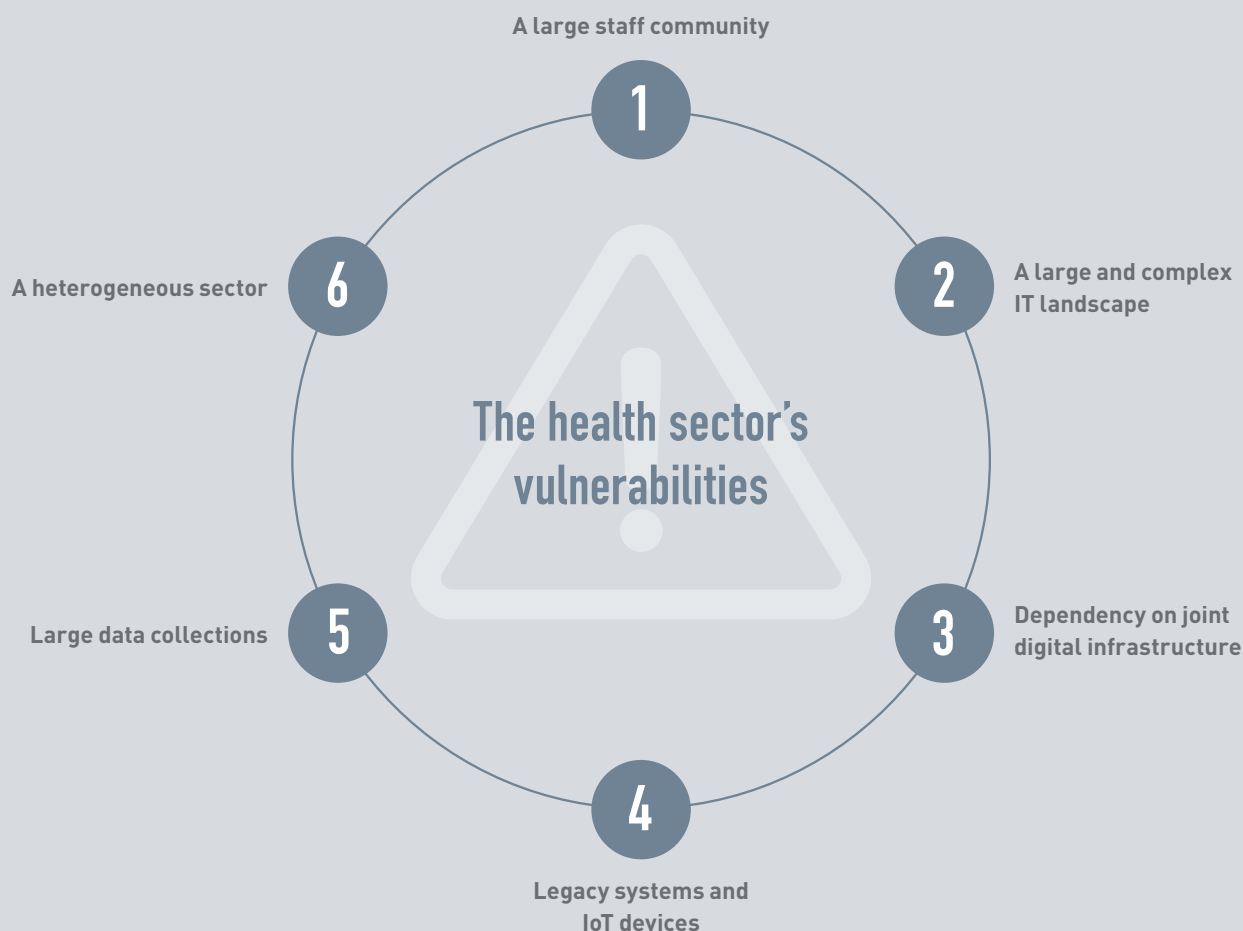
in other sectors that are critical to Danish society. Replacement is often impossible or not suitable, as critical treatment depends on the use of specific equipment. Finally, the healthcare sector uses many suppliers of both IT systems and infrastructure. Security and stability are therefore significant factors when using external suppliers in the sector. This increases the need for collective basic requirements for controlling and monitoring the security of suppliers.





FIGURE

# Six general vulnerabilities



## 1. A large staff community

The sector has several hundred thousand employees with very different preconditions regarding cyber and information security.

## 2. A large and complex IT landscape

The sector is connected through a large and complex landscape of IT systems that process sensitive personal data. This makes cyber and information security efforts a complex and extensive task.

## 3. Dependency on joint digital infrastructure

Digitally, the sector is closely interconnected by means of e.g. the Danish Health Data Network, which is used for exchanging patient data etc. A lack of confidentiality, integrity, and availability concerning these data could have major consequences for the sector and, not least, for citizens.

## 4. Legacy systems and IoT devices

Critical medical equipment may be connected to legacy systems that do not necessarily have a sufficient level of security but cannot be replaced nonetheless. At the same time, the number of a wide variety of IoT devices is increasing in the sector.

## 5. Large data collections

Large volumes of data relating to activity in the healthcare service are stored in patient records, national registries, and clinical quality databases. It is essential to maintain the confidentiality, integrity, and availability of these.

## 6. A heterogeneous sector

The healthcare sector is comprised of actors with varying levels of maturity concerning cyber and information security; everything from large, highly specialised hospitals with thousands of employees to small, private medical clinics with fewer employees.

Cyber and information security is not only about technology, but about people as well. An effective security effort also puts demands on staff expertise and skills. The many thousands of employees in the healthcare sector have very different preconditions when it comes to cyber and information security. This is why a targeted effort towards the many different professional groups in the sector is needed to ensure a consistently high level of skills and expertise regarding cyber and information security and a robust security culture across healthcare-sector actors.

**Cyber and information security  
is not only about technology,  
but about people as well.**

The challenges related to cyber and information security are many and constantly evolving. The purpose of this strategy is to support a security boost in the sector and strengthen the sector's collective ability to predict, prevent, detect, and respond to cyber and information security incidents. This requires a holistic approach and cross-sectorial coordination, as well as a collectively high level of security across the actors in the sector.

An essential component in a holistic approach is that it has to be risk-based. The healthcare sector is a critical sector, but not all processes and IT systems are equally critical to the sector as a whole. The level of security in the sector as a whole needs to correspond to the risk of cyber and information security incidents, while

also taking into account the general demands for productivity, quality, and accessibility of healthcare. It is necessary to assess where the risks are greatest and where a poten-

tial security incident would be most critical in order to prioritise security measures according to the most significant risks.

This will help ensure a holistic approach across the entire sector. The balance between managing the individual risks and the consideration for general treatment and care is also absolutely key. Ultimately, security measures should support the quality of treatment and care, including citizen trust in healthcare.





# Cyber security and information security.

## Two fields with a common aim:



### INFORMATION SECURITY

Information security is an umbrella term for the collective measures used to secure information in relation to confidentiality, integrity (amendment of data), and availability. This involves organising security work, influencing behaviour, data processing, managing suppliers, and technical security measures.



### CYBER SECURITY

Cyber security involves protection against security breaches occurring as a result of attacks on data or systems via a connection to an external network or system. Thus cyber security focuses on vulnerabilities at links between systems, including connections to the Internet.



### SECURITY FOR CITIZENS

Only an effort based on both cyber security and information security can create a foundation for citizens to feel safe regarding their treatment and health data.

# The sector is responsible for maintaining safe and secure treatment for all citizens and for preserving the confidentiality, integrity, and availability of health data

The national cyber and information security strategy emphasises that the distribution of responsibility for cyber and information security in Denmark is based on the sector responsibility principle: the authority that has the day-to-day responsibility for a given task retains responsibility in the event of a cyber and information security incident. Thus healthcare sector providers are responsible for cyber and information security in the event of an incident in the healthcare sector.







# Everyone in our sector protects citizens and their health data

---

Cyber and information security is not new to the healthcare sector. This strategy builds on a good foundation provided by the individual operators in order to further strengthen the collective efforts across the sector.

An increased awareness of cyber and information security is expressed in a number of measures throughout various parts of the healthcare sector:

With a desire to create a collective understanding of the evolving threats against the healthcare sector, the government, Danish Regions, and Local Government Denmark have established a political cyber forum at **joint public** level with the participation of the Minister of Health, the Chair of Danish Regions, and the Chair of Local Government Denmark's Health and Elderly Committee. The purpose of this forum is to discuss political considerations regarding cyber and information security and to ensure mutual orientation, knowledge-sharing, and knowledge-building to enhance the collaboration on cyber and information security in the healthcare sector.

At **state** level, the Ministry of Health works systematically with enhancing cyber and information security, including the implementation of awareness campaigns, certification of staff, and regular security tests and emergency response exercises. Emphasis is also placed on a high level of cyber and information security as part of the establishment of the Danish National Genome Centre as well as the Health Data Platform (Sundhedsdataplatformen), which is to support the Danish Health Data Authority's current and future needs for receiving, storing, and providing health data. Among other things, data is always processed anonymously so it cannot be traced immediately back to an identifiable natural person.

The **regions** have devised a political line for information security as part of the regional Health Data initiative. In continuation of this political line, the regions have approved a joint regional information security policy that supports their compliance with ISO 27001. Furthermore, the regions have prepared an interre-

gional benchmark for information security that supports the implementation of the political line and ensures a collective approach to the information security and data protection efforts in the regions. Work on the benchmark's crossregional deliveries has contributed to further enhancement of the efforts and the professional level in each region by means of, for example, common frameworks, guidelines, and feedback. In continuation of the benchmark, a permanent interregional steering committee for information security has been set up. Parallel to this, each individual region is



working to ensure that information security is permanently made an integral part of the services provided to citizens, patients, enterprises, partners, and others.

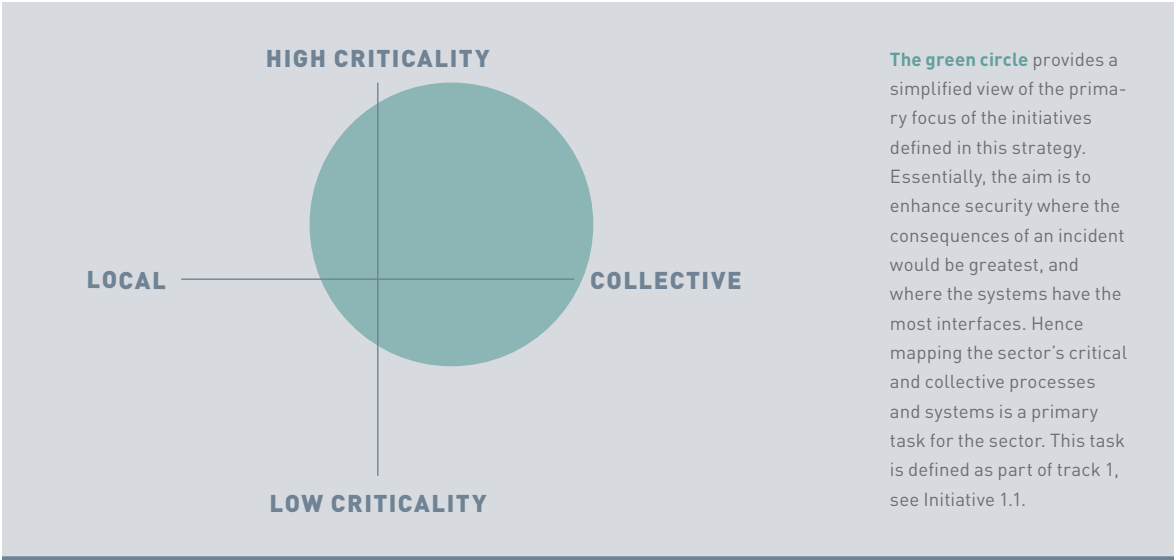
At a **municipal** level, the Security Programme (Sikkerhedsprogrammet) has been established as part of the joint municipal digitisation strategy. This programme aims to support the work of the 98 municipalities on enhancing security for all areas in the municipalities, including implementation of the principles of ISO 27001 and the development of the municipalities' joint framework for IT architecture with an emphasis on data security. Moreover, the programme aims to support greater awareness of data security among municipal managers and staff alike. To support and ensure continuous emphasis on information security in the individual municipalities, Local Government Denmark is conducting an annual analysis of the municipalities' maturity levels with regard to security until 2020. This has led to insights about which areas are most advantageous to collaborate on, where Local Government Denmark can support the efforts of the municipalities. Among other things, the results of the analysis have led to the allocation of more funds towards increasing the awareness of information security among employees within the individual municipalities. This analysis has also resulted in a build up of expertise regarding municipal information security and associated legal functions.

**The strategy aims to ensure that the healthcare sector's cyber and information security efforts are coordinated and aligned across healthcare actors.**

Within **primary healthcare** the Danish Organisation of General Practitioners is supporting a general increase in information security awareness among general practitioners. In 2017 the organisation compiled information material about the legal responsibilities of general practitioners, as well as guidelines on relevant security behaviour regarding the protection of IT systems and personal data. This was followed up in 2018 by awareness activities aimed directly at general practitioners.

On the basis of the existing efforts, the strategy will enhance the sector's overall capacity related to cyber and information security. The strategy aims to ensure that the healthcare sector's cyber and information security efforts are coordinated and aligned across healthcare actors, including strengthening knowledge-sharing across the healthcare sector. The strategy also aims to create greater transparency regarding the roles and responsibilities of the individual healthcare actors; in terms of their day-to-day work, but also in the event of security incidents. Furthermore, the strategy ensures that the effort is given priority and that it is continuously developed so that the security level and the security measures of the healthcare sector match the continuous evolution of new kinds of security incidents.

**FIGURE** Mapping of the sector's critical and collective processes and systems







# We are already enhancing security

In the healthcare sector, a general capacity-building in relation to cyber and information security is currently underway. This includes compliance with ISO 27001 and the EU's regulation in the field in the form of the Directive on security of network and information systems (the NIS Directive) and the General Data Protection Regulation (GDPR).

## **EU Directive on security of network and information systems (the NIS Directive)**

The NIS Directive came into force on 9 May 2018 with the aim to enhance security in services dependent on network and information technology. Thus the healthcare sector must operate in compliance with the directive's requirements regarding the reporting of security incidents and the designation of operators of essential services.

## **EU General Data Protection Regulation (GDPR)**

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and includes a long series of provisions that aim to guarantee the protection of personal data. Among other things, the GDPR places an emphasis on privacy by design and by default, and it provides the opportunity to impose considerable penalties on authorities and companies in the

event of a breach of data security. A hospital in Barreiro, Portugal was among the first organisations subject to a penalty under the auspices of the GDPR. The penalty of EUR 400,000 was due to the fact that the hospital did not have appropriate measures in place to limit staff access to patient data, and that the hospital did not sufficiently secure the confidentiality, integrity, availability, and resilience of its IT systems.

## **The actors in the healthcare sector agree to comply with ISO 27001**

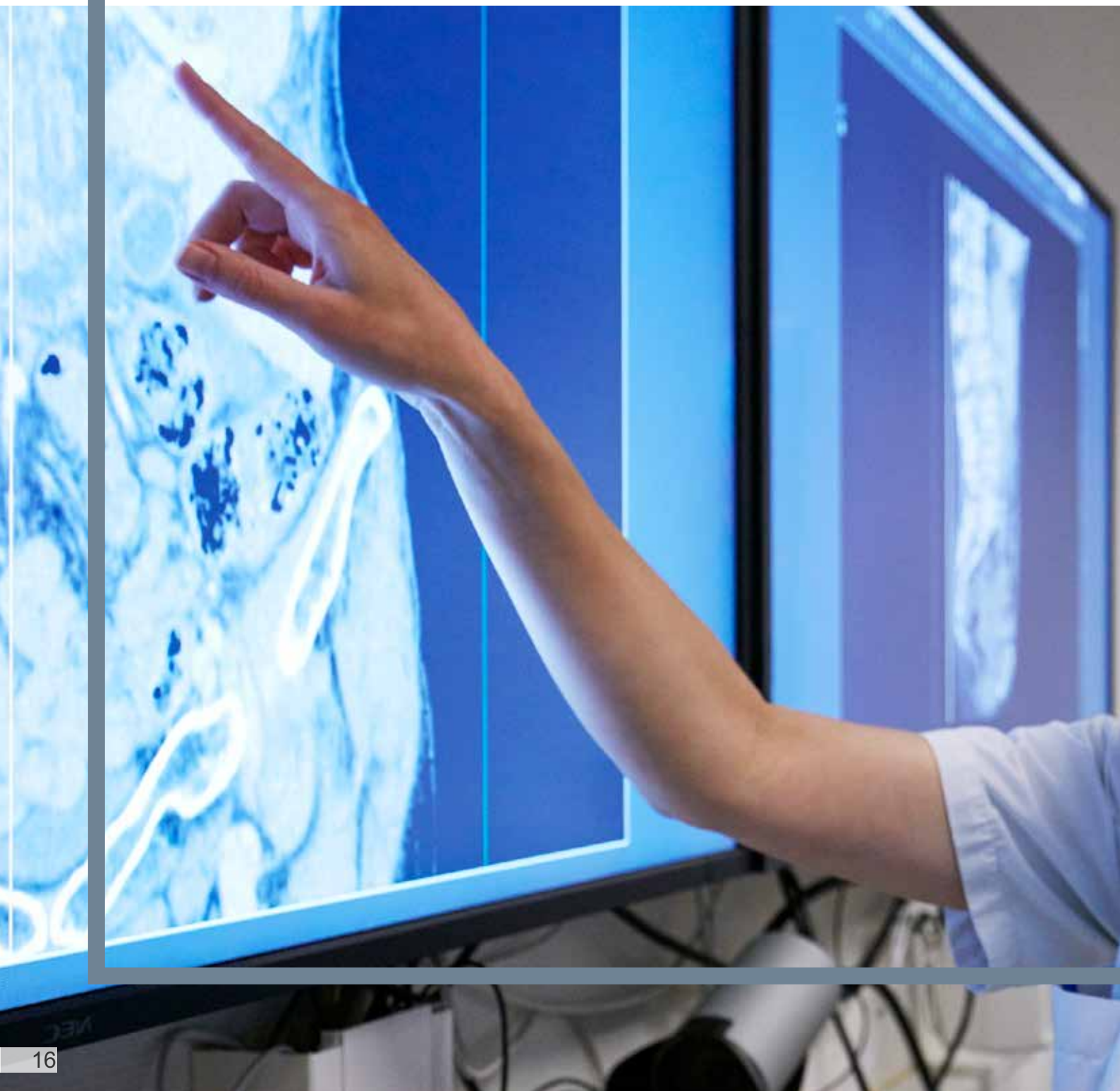
Compliance with ISO 27001, an international standard for information security management, is mandatory for all state authorities in Denmark. Similarly, the regions have chosen to comply with ISO 27001 and the municipalities have agreed to meet the principles of the standard. In preparation of the strategy and its initiatives, the healthcare sector has also been inspired by the National Institute of Standards and Technology's (NIST) framework for cyber security. The threats are dynamic, and therefore it has been necessary to supplement the emphasis on management and processes in the mandatory ISO 27001 with a number of faster, more agile and technical measures in order to support a holistic enhancement of the capacity of the sector concerning cyber and information security.

## → The national strategy defines the remits

The Danish National Strategy for Cyber and Information Security 2018-2021 instructs the healthcare sector – in parallel to five other critical sectors (energy, finance, maritime, telecommunication, and transportation) – to devise a sector-specific strategy for cyber and information security and establish a decentralised cyber and information security unit (DCIS) in the sector. With the publication of this strategy and the establishment of the decentralised cyber and information-security unit (DCIS) for the Danish healthcare sector in Danish Health Data Authority, these requirements are met. Likewise, the strategy's initiatives meet other requirements defined in the national strategy.

BACKGROUND AND ANALYSIS

# Threats, vulnerabilities, and risks in the healthcare sector



Cyber and information security in the healthcare sector is associated with various different threats, vulnerabilities, and risks. The combination of technological development and innovative opponents makes cyber and information security a complex and dynamic challenge. This is a field in a state of flux.



# The threat pattern is both complex and constantly changing

The healthcare sector and its tasks and procedures are constantly evolving – among other things, as a consequence of the digitisation of the healthcare service and the fact that treatment and care tasks are presently being placed closer to the citizens. At the same time, the threat pattern is constantly evolving.

In July 2018, the Danish Centre for Cyber Security published the first sector-specific threat assessment for the Danish healthcare sector. Based on international experiences, the Danish Centre for Cyber Security points out that the threats against the healthcare sector may come from a number of different actors – both state actors and criminals – and may take many different forms; from espionage to ransomware and phishing emails.

However, cyber and information security in the healthcare sector cannot be reduced to protecting the sector from hostile external actors only. Alongside the Danish Centre for Cyber Security's threat assessment, the work on this strategy has also included the compilation of a vulnerability assessment in order to map and assess the various vulnerabilities in the Danish healthcare sector. In general, the vulnerability assessment points out a number of vulnerabilities in the healthcare sector that it is particularly important to address; including legacy systems and equipment, supplier management, the mutual dependencies of healthcare actors related to the interaction of the various technologies, and cyber and information-security expertise among the many different groups of employees in the sector.

The healthcare sector is critical for society, and by definition many of the sector's processes and IT systems are critical. However, not all of them are equally critical for the sector as a whole. Thus the processes and systems included directly in the treatment and care of citizens and the handling and storage of their personal data are simply more critical than the processes and systems that support the administrative work in the sector. For example, if the sector's laboratory systems or imaging diagnostics are affected, this is more critical than if the sector's processes and systems for settlement and payments are affected. In the same way, processes and systems used and run by a number of the sector's actors are also more critical than systems that are only used locally by a single actor.

On the basis of the sector's vulnerability assessment and the Danish Centre for Cyber Security's threat assessment, a collective risk assessment has therefore been compiled for the healthcare sector in order to ensure a holistic, risk-based approach to cyber and information security. Here the consequences for the healthcare sector have been assessed for the various risks: this helps to prioritise the sector's efforts towards the biggest risks and most critical processes and systems. Moreover, the risk assessment helps to determine the appropriate security level in relation to the risk in question, taking into consideration both the consequences of an incident and the general treatment and care of citizens.

## → The CfCS assesses that the threat from

- cyber espionage against the Danish healthcare sector is **very high**
- cybercrime against the Danish healthcare sector is **very high**
- cyber activism against the Danish healthcare sector is **low**
- cyber terrorism against the Danish healthcare sector is **low**

FIGURE

## The strategy is based on continuous analyses and conclusions











# The WannaCry attack and the British healthcare service

The high level of digitisation in the healthcare sector entails a greater vulnerability to cyber and information security incidents. For example, in May 2017 the National Health Service (NHS) in the UK was affected by ransomware. This was part of what was known as the WannaCry attack, which infected several hundred thousand computers all over the world. WannaCry rendered a wide range of systems unavailable and resulted in more than 19,000 cancelled treatments and the need to redirect many patients. In total, it is estimated that WannaCry cost the NHS around £92 million.

# Four tracks for the enhancement of cyber and information security

---

For the healthcare sector to be able to withstand and manage both current and future threats and risks, there is a need for cross-sectorial enhancement of the entire collective cyber and information security effort. Therefore the strategy is divided into four tracks: the strategy aims to strengthen the healthcare sector's capacity to predict, prevent, detect, and respond to cyber and information security incidents. A number of specific initiatives have been designated for each track, and the actors in the sector will work together to implement them. Some of the initiatives build on existing efforts among some of the

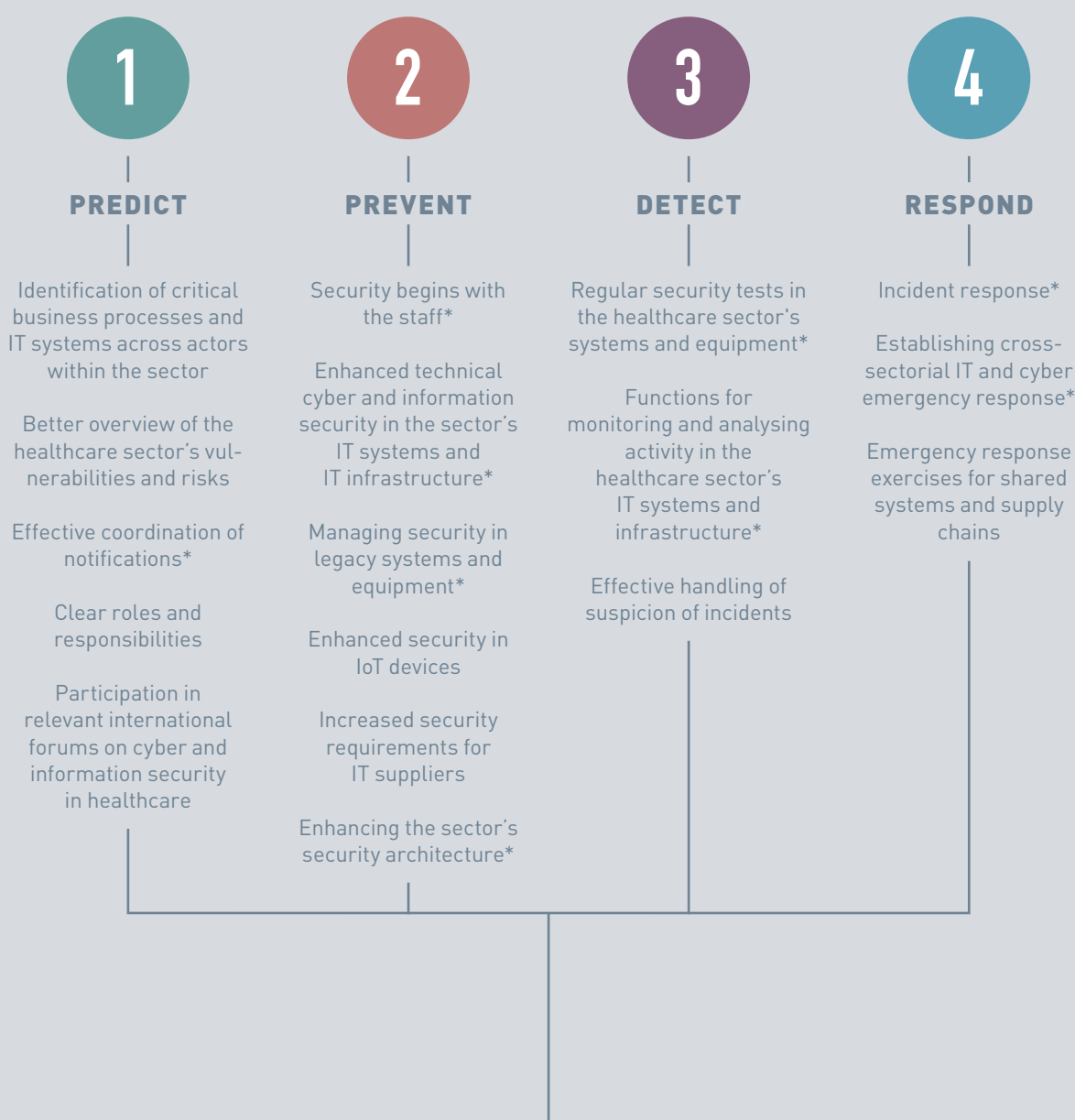
## **All aspects of cyber and information security are addressed and assessed.**

actors, while others involve new joint measures. Furthermore, some of the strategy's initiatives aim to bring together a number of activities in the sector to form cross-sectorial activities via the healthcare sector's decentralised cyber and information security unit (DCIS) in the Danish Health Data Authority.

The aim of this approach is to ensure a holistic approach to the collective efforts towards strengthening the collective level of security in the healthcare sector and ensure that all aspects of cyber and information security are addressed and assessed.



# A coherent and systematic approach to strengthened security

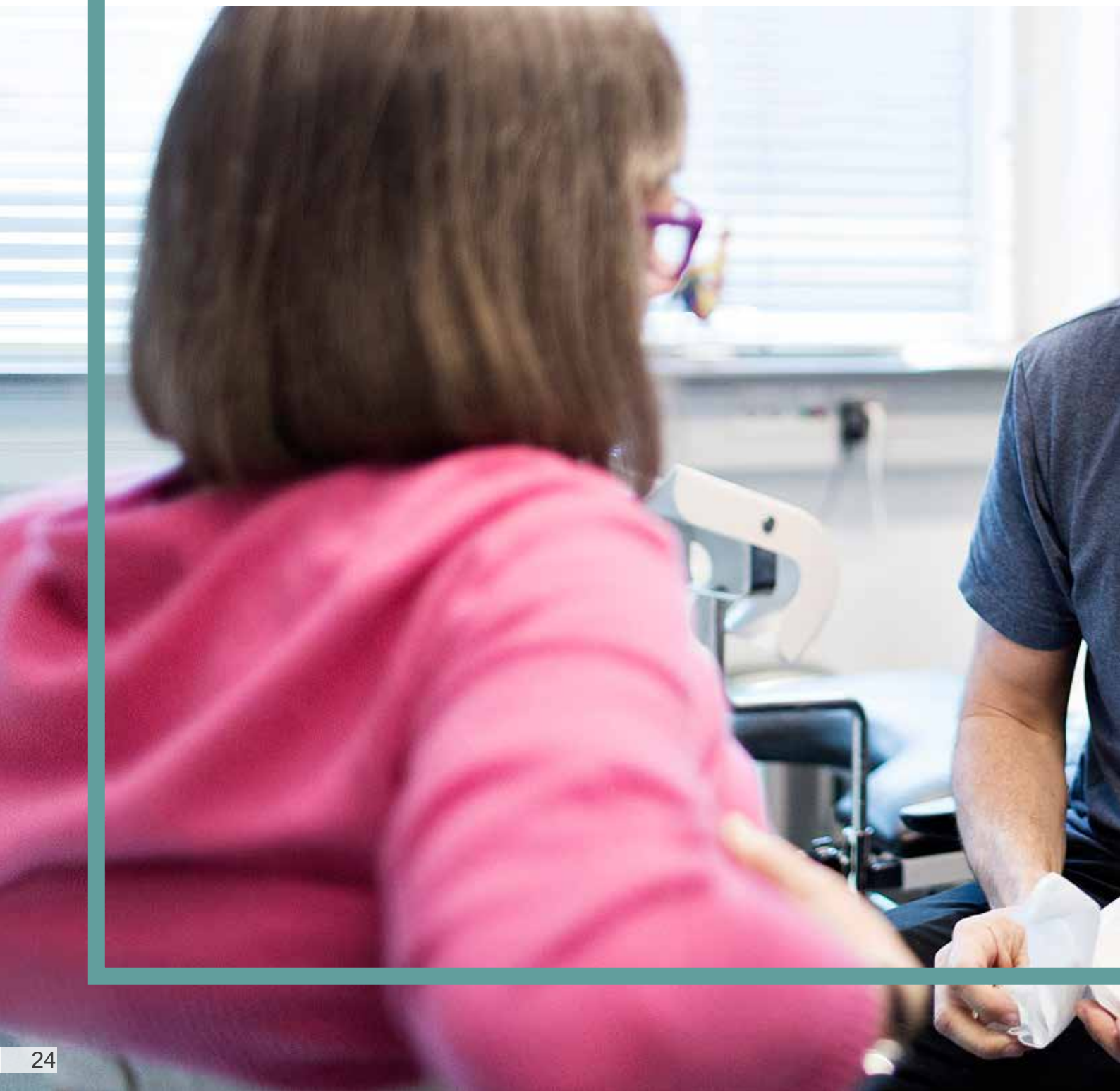


## Implementation and organisation

\*Initiatives where one or more activities require additional agreements on funding.

TRACK 1 - PREDICT

# Better prediction of potential attacks and incidents





Better prediction of potential cyber and information security incidents is crucial to the timely and effective implementation of the right security measures at the right levels. This is a significant prerequisite for ensuring that the sector as a whole and the individual actors will be able to make the right decisions on the necessary security level.



# In many instances potential attacks and incidents can be predicted

The ability to predict potential cyber and information security incidents is conditional on a number of things – among other things: knowledge of critical processes and systems, an overview of vulnerabilities and risks, rapid and effective dissemination of notifications of potential and imminent security incidents to all relevant actors, a clear distribution of roles and responsibilities, and sharing the latest knowledge in the field with relevant international partners.

On this basis, the strategy must ensure that the healthcare sector as a whole generates a more precise description of the sector's critical processes, systems, and mutual dependencies, along with a more collective and consistent understanding of the vulnerabilities and risks, as well as roles and responsibilities associated with these risks.

**For example, information about attacks abroad that may affect the healthcare service in Denmark can be used as a basis.**

The Danish Centre for Cyber Security's threat assessments for the sector must be accompanied by vulnerability and risk assessments both for the sector as a whole and for the individual actors on the basis of ISO 27001.

At the same time, the strategy must ensure that all relevant actors in the sector receive faster and more precise notifications in the event of, for example, attacks abroad to ensure that they have a

clear picture of the current threats and are able to take the right precautions. This should be enhanced by establishing clear, secure lines of communication – both between the healthcare sector and the Danish Centre for Cyber Security, and across all actors within the sector.

## → It is important that threat assessments are disseminated



The Danish Centre for Cyber Security compiles assessments of cyber threats specifically against the healthcare sector. This supports the healthcare sector's cyber and information security efforts. It is essential that all relevant actors in the healthcare sector receive timely and effective information about updated threat assessments to ensure that local action can be taken accordingly. The decentralised cyber and information security unit (DCIS) in the Danish Health Data Authority will therefore cooperate with the rest of the sector on establishing procedures for how the sector's actors will receive information about threat assessments.



## → Initiatives

1

**Identification of critical business processes and IT systems across actors within the sector**

2

**Better overview of the healthcare sector's vulnerabilities and risks**

3

**Effective coordination of notifications**

4

**Clear roles and responsibilities**

5

**Participation in relevant international forums on cyber and information security within healthcare**

#### INITIATIVE 1.1.

---

### Identification of critical business processes and IT systems across actors within the sector

To ensure a focused approach to cyber and information security it is necessary to identify the sector's most critical business processes and the IT systems that support them. With input from healthcare-sector actors the DCIS facilitates an annual review of the sector's critical business processes, IT systems, and supply chains. The first version will be compiled by the first half of 2019.

#### INITIATIVE 1.2.

---

### Better overview of the healthcare sector's vulnerabilities and risks

Local and cross-sectorial assessments of vulnerabilities and risks within the healthcare sector must be maintained continuously. Each individual actor is responsible for compiling and updating its own vulnerability and risk assessments and for ensuring management support. Together with sector actors the DCIS will compile guidelines supporting this work in 2019 with the aim that assessments across the sector will become methodologically consistent over time. Moreover, it will be mandatory to follow these guidelines for assessments of shared, prioritised, and critical systems. The DCIS has also been tasked with compiling the overall vulnerability and risk assessment for the entire sector.

#### INITIATIVE 1.3.

---

### Effective coordination of notifications

The sector's ability to predict potential attacks and security incidents will be enhanced by the establishment of an overall model for effective coordination of notifications about potential threats and security incidents. This will be implemented by the DCIS in the first quarter of 2019. This will include a first version of a function for receiving and submitting notifications, subscriptions, rules for the distribution of alerts, etc. This ensures that all relevant actors receive quick and precise information about a potential attack in progress, allowing them to take the right precautions. The function will be implemented by sector actors and covered by their own budgets. The establishment of an extended solution requires specific agreement for this part.

#### INITIATIVE 1.4.

---

### Clear roles and responsibilities

Awareness of one's own role and responsibility in relation to cyber and information security is crucial if every actor in the healthcare sector is to be able to react quickly and effectively in the event of cyber and information security incidents. An initial description of the individual stakeholders' roles and responsibilities across the sector has been compiled as part of the strategy process. The DCIS has been tasked with developing this description further in the first half of 2019, as well as with maintaining clear roles with the involvement of sector actors. The DCIS should also ensure that all actors involved are familiar with their individual roles and responsibilities.

#### INITIATIVE 1.5.

---

### Participation in relevant international forums on cyber and information security in healthcare

Cyber and information security, as well as the potential measures to counter a changing threat pattern, are undergoing rapid development. It is therefore crucial for the healthcare sector's cyber and information security effort that it is based on the latest international expertise, including trends in technology, methods of analysis, etc. The DCIS should therefore identify and participate in relevant international forums on cyber and information security in healthcare. The DCIS should also engage in networking activities with relevant cyber and information security units in healthcare. The DCIS will ensure that relevant knowledge from this network is passed on to healthcare-sector actors.



**INITIATIVE 1.4.**

Awareness of one's own role and responsibility in relation to cyber and information security is crucial if every actor in the healthcare sector is to be able to react quickly and effectively.

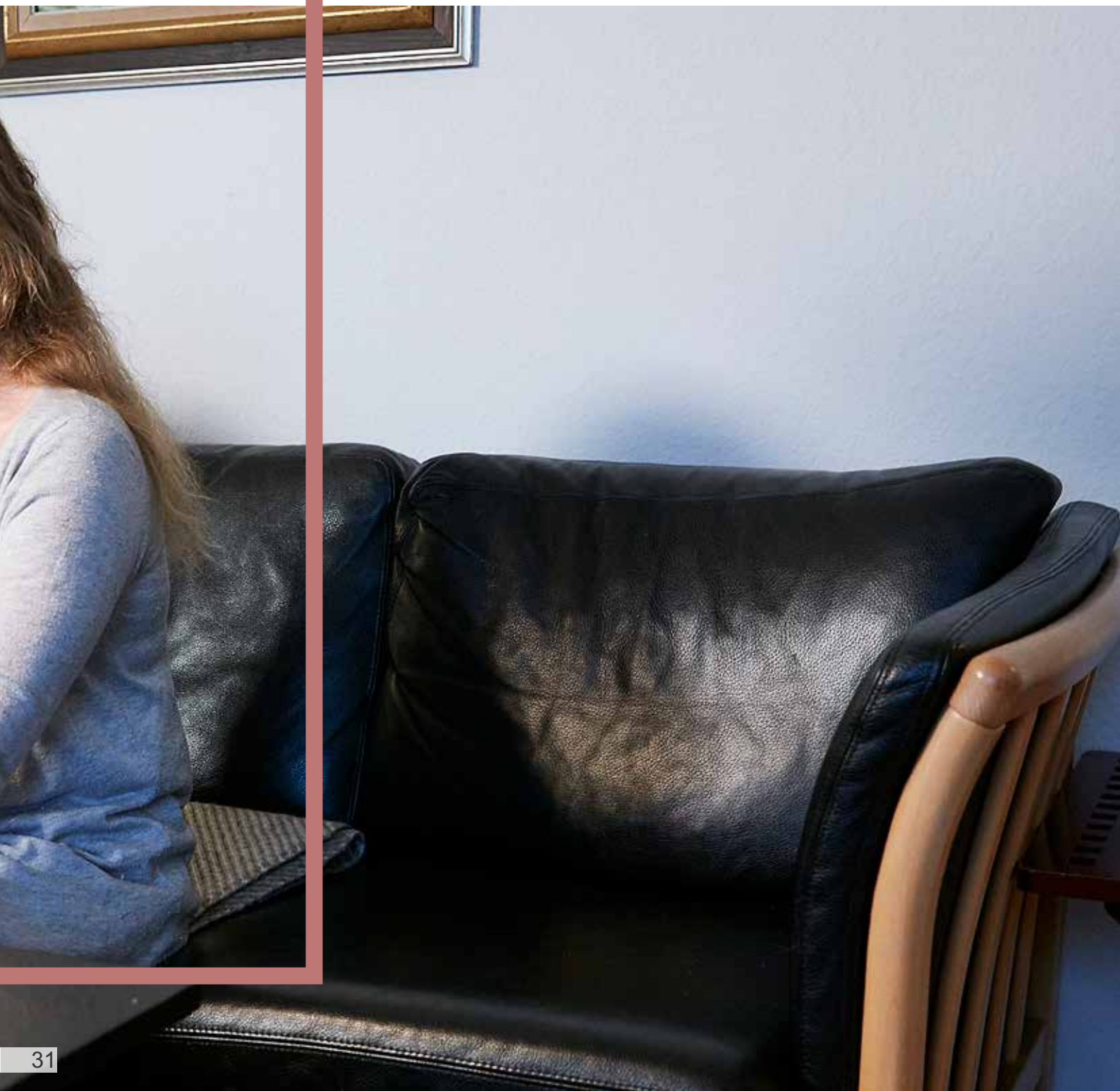
TRACK 2 - PREVENT

# Better prevention of attacks and incidents





The ability to prevent cyber and information security incidents depends on a wide range of factors – technical, organisational, human, etc. – all of which have to be in place if the risk of an unwanted incident is to be mitigated effectively.



# Effective prevention is very much a matter of culture

To ensure effective prevention it is absolutely crucial to have a strong, robust cyber and information security culture throughout the entire sector. This includes ensuring that staff have the necessary knowledge and skills in relation to cyber and information security, so sensitive personal data is handled appropriately and securely and staff are alert to, for example, phishing emails and other types of attempted attacks.

Of course, technical security measures are also important to our efforts to prevent cyber and information security incidents, but without staff awareness and understanding of the need for these measures there is a potential risk that staff will inadvertently circumvent technical security during a busy work day. Therefore additional cyber and information security training for the various groups of staff in the health-care sector should contribute to staff awareness and appropriate security behaviour.

In addition to awareness activities, the strategy also entails a number of other initiatives to enhance the sector's ability to prevent cyber and information security incidents. On the basis of a risk-based approach,

the right technical security measures must be implemented both locally and in shared IT systems to prevent attacks and security incidents.

As part of enhancing technical security in the sector, it is also necessary to deal with the challenge presented by legacy systems. Many of these systems do not necessarily live up to current security standards. Notwithstanding, it may be difficult or inexpedient to replace or update them, as they are often necessary

for treatment. IoT devices connected to the internet represent a further challenge in this regard.

To strengthen the prevention efforts across the sector, health-

care sector parties will work on a set of shared basic security requirements to be used in contracts with suppliers providing IT solutions and IT operations for the sector. These shared supplier requirements will be based on the work with supplier contracts, which has been initiated as part of the national strategy for cyber and information security. In addition, health-care-sector actors will work together to expand and enhance the sector's security architecture by, for example, increasing the focus on privacy by design.

**Effective prevention requires a strong cyber and information security culture throughout the entire sector.**

## → Security policies



Each and every actor in the healthcare sector must have applied security policies and specific guidelines aimed at their staff and processes. Security policies must be updated corresponding to the needs and developments in the threat pattern.



## → Initiatives

1

**Security begins with the staff**

2

**Enhanced technical cyber and information security in the sector's IT systems and IT infrastructure**

3

**Managing security in legacy systems and equipment**

4

**Enhanced security in IoT devices**

5

**Increased security requirements for IT suppliers**

6

**Enhancing the sector's security architecture**

## INITIATIVE 2.1.

### Security begins with the staff

A high level of awareness among healthcare-sector staff with regard to the risk of cyber and information security incidents is a key factor in the efforts to strengthen the sector's ability to prevent potential cyber and information security incidents. Therefore all staff in the healthcare sector must receive training on cyber and information security; either through, for example, the training packages developed under the auspices of the public-sector Digital Strategy 2016-2020 or through local initiatives. Moreover, the DCIS will contribute to the ongoing efforts to strengthen the focus on cyber and information security in relevant training programmes, including courses within healthcare degree programmes. Moreover, awareness of cyber and information security should be enhanced at all management levels, and it is necessary to ensure that the staff who work specifically with cyber and information security in the healthcare sector have the right skills. The implementation of cross-sectorial activities as part of this initiative requires an additional agreement between sector parties.

## INITIATIVE 2.2.

### Enhanced technical cyber and information security in the sector's IT systems and IT infrastructure

Technical cyber and information security in the healthcare sector's IT infrastructure must be enhanced by establishing appropriate and up to date technical arrangements to increase the sector's capacity to protect data and systems and prevent cyber and information security incidents. To this end, a number of mandatory technical requirements have been inserted into the template for the shared public-sector data processing agreement for healthcare. In addition, as part of the national objective to achieve end-to-end encryption in the healthcare sector's IT infrastructure, an initiative targeted at end-point encryption (or justified opt out) is being implemented in the regions' services presented via the Danish Health Data Network. Furthermore, the purchase and commissioning of new technology must be planned ahead in order to support the sector's strategic and risk-based approach to new technology.

## INITIATIVE 2.3.

### Managing security in legacy systems and equipment

Healthcare-sector actors must deal with security in legacy systems and equipment that fail to meet current security standards. In the second half of 2019 the DCIS will therefore facilitate a mapping of the sector's legacy systems and equipment on the basis of a risk-based approach and with particular emphasis on IT systems identified as shared critical systems. Further joint activities within this initiative require additional agreements between healthcare-sector parties.

### → General IT-operating hygiene is a significant factor

General IT-operating hygiene is an essential foundation for cyber and information security efforts. Of course, this cannot stand alone against an elevated level of threats, but it is crucial to keep track of the day-to-day IT operation and to have basic processes and procedures in place to ensure that there is a good and robust starting point for the remaining cyber and information security work. It is important that individual healthcare-sector actors document and use well-defined, tried and tested processes for, for example, procurement of new systems, further development and maintenance of existing IT systems, and updates and configuration changes. General IT-operating hygiene includes recognised methods for, for example, life-cycle management and change management. This helps to ensure that a consistently high and robust security level is maintained at all times.



**INITIATIVE 2.1.**

A high level of awareness among healthcare sector staff with regard to the risk of cyber and information security incidents is a key factor in the efforts to strengthen the sector's ability to prevent cyber and information security incidents.





#### INITIATIVE 2.4.

### Enhanced security in IoT devices

Security in the sector must be enhanced in relation to IoT devices connected to a network. Initially, the Danish Medicines Agency and the DCIS will initiate a strategic partnership in 2019 to share relevant knowledge, discuss the latest regulatory requirements in the field, etc. Furthermore, the Danish Centre for Cyber Security will publish an assessment of the cyber threats specific to medical equipment connected to a network in 2019. Moreover, the DCIS is making it easier for the sector's actors to share knowledge and experiences, including best practices for the handling of medical equipment.

#### INITIATIVE 2.5.

### Increased security requirements for IT suppliers

Healthcare-sector actors use private suppliers to a great extent for, for example, the procurement and development of new technology, while parts of the healthcare sector's IT systems are run by either private suppliers or by a public actor on behalf of the entire sector. To ensure that private and public IT suppliers are met with consistent requirements with regard to a high level of security from all sector actors, collective security requirements must be compiled, along with processes and tools to support compliance with these requirements. This initiative will commence in the second half of 2019. The public-sector clause library is one of the starting points. MedCom will also carry out an analysis of the prospects of implementing supplier management via, for example, the Danish Health Data Network.

#### INITIATIVE 2.6.

### Enhancing the sector's security architecture

Efforts must be made to work with consistent requirements for IT security across the healthcare sector, e.g. regarding privacy by design and in relation to further development of existing systems or new procurements. The sector must commit to a shared set of methodologies and standards that are applicable to the entire sector. The aim of this is to ensure an appropriate and consistently high level of privacy by design and by default. As a basis for this, the DCIS is tasked with updating the overall security architecture for the sector, including the establishment of standards and the preparation of tools and guidelines. This initiative will commence in the second half of 2019. Pilot-testing of the new security architecture requires an additional agreement between healthcare-sector parties.

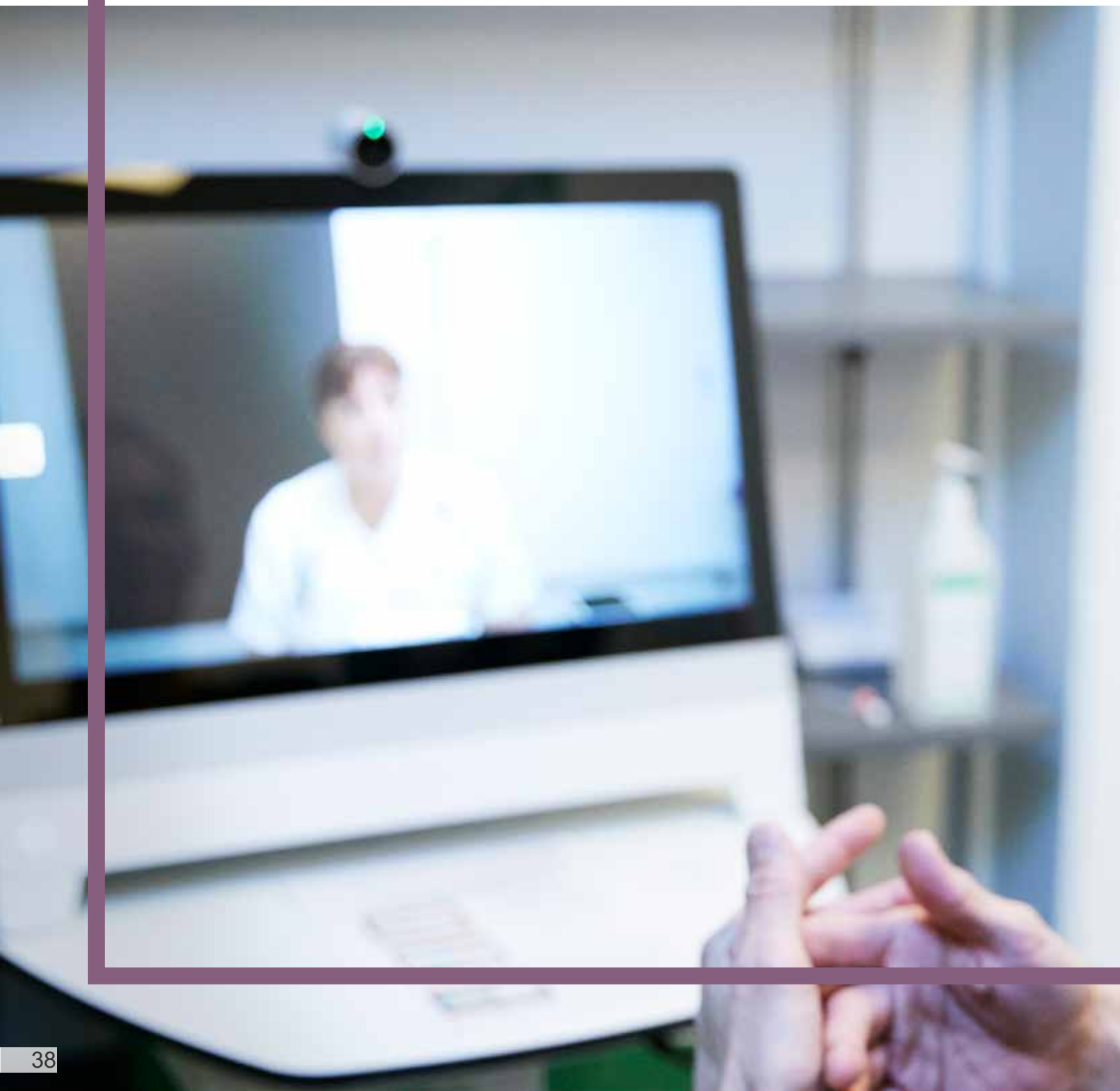
## → Cyber defences that work

To strengthen cyber and information security in an organisation a range of basic measures should be implemented. In the publication *Cyber Defences that Work* (Cyberforsvar der virker) the Danish Centre for Cyber Security and the Danish Agency for Digitisation outline seven steps towards good cyber defences, including management support, technical skills, awareness, and four basic security measures:

- **Compile a whitelist of applications**
- **Update software**
- **Update operating systems**
- **Limit the number of user accounts with domain or local administrative privileges**

TRACK 3 - DETECT

# Better detection of attacks and incidents



In addition to better prediction and prevention of cyber and information security incidents, the health-care sector must build the capacity to detect imminent incidents and attacks – if, for example, an unauthorised external actor has gained access to the sector’s IT systems.



# It is a matter of intelligent monitoring and everyday awareness

To support the detection of attacks and security incidents it is necessary for the actors in the sector to proactively monitor activity on both shared and local IT infrastructure and IT systems. This requires that the appropriate monitoring functions are in place in the right places in the sector, and that the sector is well-coordinated in this regard in order to enhance its capacity to detect breaches of cyber and information security across actors in the sector. With a collectively high level of security, the sector will enhance its collective resistance to attacks and security incidents.

As a next step, it is important that the healthcare sector's monitoring functions are coordinated with lines of communication, emergency response, and contingency plans in the sector. Naturally, this is also applicable across the sectors regarded as critical to Danish society, as well as across national borders to healthcare sectors in countries with which we cooperate regarding cyber and information security alerts and notifications. In the event of an incident, the incident needs to be rapidly detected and contained to ensure that it does not spread within or across sectors.

Cyber and information security is continuously evolving. The threat pattern is changing rapidly, and new

forms of attack are constantly emerging. The sector's capacity to detect new forms of cyber and information security incidents must keep up with this development, and the sector's monitoring functions must measure up to both the current threat pattern and the risks the threats pose to citizens, healthcare professionals, and society in general. Therefore the actors in the sector should carry out regular security tests of both the shared and the local infrastructure to ensure that new vulnerabilities and security flaws are detected and managed.

Detection of new vulnerabilities and security flaws is also dependent on the vigilance of both the sector's own staff and external actors, such as ethical hackers. The sector must therefore be ready and have procedures in place for dealing with enquiries from staff and other members of the public concerning potential vulnerabilities in the sector's IT systems or regarding suspicions of security breaches.

Overall, these measures will strengthen the sector ability to both deal with these challenges and become aware of changing patterns in cyber and information security incidents, as well as to notify relevant parties of an ongoing threat.

**With a collective and high level of security the sector will enhance its collective resistance to attacks and security incidents.**

## → MedCom and Sundhed.dk are already enhancing security

The healthcare sector is already working on initiatives to enhance security across the sector. MedCom has implemented a new version of the Danish Health Data Network that further enhances security. The Danish Health Data Network provides the foundation for the majority of digital communication across the healthcare sector. Similarly, Sundhed.dk – the primary point of access to their own health data across the sector for many citizens – maintains a high level of security by means of recurring security tests, monitoring connected systems, and repeated security reviews of associated apps, processes, and procedures, as well as the infrastructure used in relation to the portal.





### TRACK 3 - DETECT

## → Initiatives

1

**Regular security tests in the healthcare sector's systems and equipment**

2

**Functions for monitoring and analysing activity in the healthcare sector's IT systems and infrastructure**

3

**Effective handling of suspicion of incidents**

### INITIATIVE 3.1.

## Regular security tests in the healthcare sector's systems and equipment

For the healthcare sector as a whole to be able to maintain robustness against cyber and information security incidents, it is necessary to carry out regular security tests of the healthcare sector's IT systems and equipment. The DCIS has been tasked with analysing whether the sector's existing test activities should be extended and possibly even assembled in an actual test programme. This may include vulnerability scans, penetration tests, and red team tests. The establishment of a test programme – including a platform for confidential disclosure of test results etc. – requires an additional agreement between healthcare-sector parties. The DCIS should also clarify the prospects of cooperating on major security tests with other sectors critical to Danish society.

### INITIATIVE 3.2.

## Functions for monitoring and analysing activity in the healthcare sector's IT systems and infrastructure

The healthcare sector must be capable of effectively detecting both local and cross-sectorial cyber and information security incidents. Thus there is a need for regular monitoring and analysing activity on both the shared and the local IT infrastructure to detect and manage unauthorised or irregular activity. As an initial activity, the DCIS will work with the actors in the healthcare sector to clarify the need for and potential of establishing joint functions for monitoring and analysing activity. This analysis should lead to decisions about how best to establish these functions.

### INITIATIVE 3.3.

## Effective handling of suspicion of incidents

The actors in the healthcare sector may experience incidents where staff – healthcare professionals and IT technicians, for example – or external actors suspect that a cyber or information security incident may have taken place or that an incident is about to take place. To ensure that actors in the sector are capable of reacting quickly and effectively to any such suspicion, clear procedures for receiving and dealing with enquiries about potential cyber and information security incidents must be put in place for each healthcare-sector actor. Costs incurred to this end will be kept within the budgets of each actor.

### → What is a red team test?

Red team tests test an organisation's cyber and information security and preparedness by means of scenario-based attacks from so-called ethical hackers (or white hat hackers), who take on the role of the hostile actors and attempt to find a way into the organisation. Unlike vulnerability scans and penetration tests, for example, tests of this type focus not only on the technical attack surface but on all cracks in the defences, thereby also testing other parameters, such as the organisation's physical security and staff awareness.



#### **INITIATIVE 3.1**

It is necessary to carry out regular security tests of the healthcare sector's IT systems and equipment.



TRACK 4 – RESPONSE

# Rapid response in the event of attacks and incidents





If, despite predictive and preventive initiatives, security is nevertheless compromised due to, for example, a cyber attack or an accidental breach of information security, the sector must be able to rapidly restore systems and return to normal, so that patient treatment can be resumed.



# It is a matter of skills, tools, and the right organisation

In the event of a potential cyber and information security incident, the incident must be handled quickly, effectively, and precisely to ensure minimum impact on the sector's everyday tasks. The incident must be contained and isolated to limit the damage and ensure that the other systems and functions in the sector are affected as little as possible.

The actors in the sector must work both jointly and locally to undertake incident and emergency response in relation to cyber and information security incidents. In this regard, the existing emergency response within the healthcare sector

constitutes a robust, tried, and tested foundation on which to build further. However, it is also necessary to strengthen the sector's capacity as a whole when it comes to managing cyber and information security incidents by means of the right skills and tools. This should help to bring about an enhanced, coordinated effort regarding both the response to specific security incidents, as well as cross-sectorial emergency response to ensure that the confidentiality, integrity, and availability of the implicated systems and data can be restored.

**The incident must be contained and isolated to limit the damage and ensure that the other systems and functions in the sector are affected as little as possible.**

A significant element in this regard is tried and tested lines of communication so that the actors in the sector know who and where to address their enquiries, as well as what can be done locally in the event of an incident. As part of this, healthcare-sector actors, as well as their staff, must have a common understanding of tasks and responsibilities, along with specific and well-

established agreements about the handling of cyber and information security incidents.

It is crucial to ensure learning. The sector's handling of incidents and emergency response needs to be constantly enhanced and kept up to date with

new threats and risks. Learning should take place in the event of an incident so that all relevant actors can benefit from the experience of dealing with the incident. Learning should also take place through recurring tests of the collective emergency response. A continuous review of experiences will help to ensure that the sector is constantly strengthening its overall capacity to predict, prevent, detect, and respond to cyber and information security incidents.

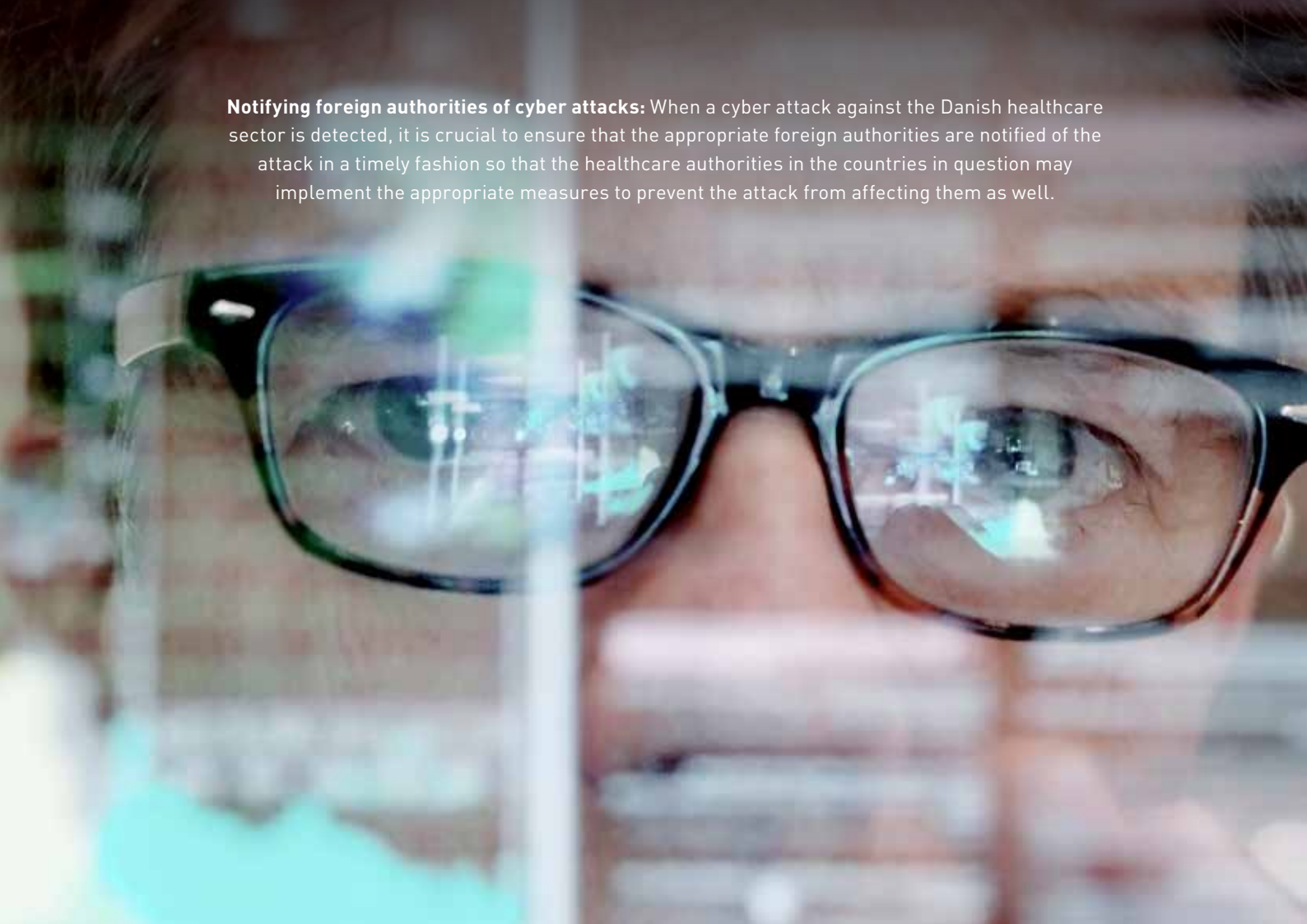
## → Reporting incidents

**In the event of a cyber and information security incident, healthcare-sector actors are, in many cases, legally bound to report the incident to the relevant authorities:**

- Pursuant to the NIS Directive, operators of essential services in the healthcare sector must report incidents with significant consequences for the continuity of the essential service as quickly as possible to the Danish Health Data Authority and the Danish Centre for Cyber Security.
- In the event of a breach of data security, healthcare-sector actors must, pursuant to the EU's General Data Protection Regulation, report the breach to the Danish Data Protection Agency without undue delay and, if feasible, within 72 hours of the data controller becoming aware of the breach.

Cyber and information security incidents must be reported via the Joint Solution for Reporting IT Security Incidents (FLIIS) at [www.virk.dk](http://www.virk.dk).





**Notifying foreign authorities of cyber attacks:** When a cyber attack against the Danish healthcare sector is detected, it is crucial to ensure that the appropriate foreign authorities are notified of the attack in a timely fashion so that the healthcare authorities in the countries in question may implement the appropriate measures to prevent the attack from affecting them as well.

#### TRACK 4 - RESPONSE

## → Initiatives

1

**Incident response**

2

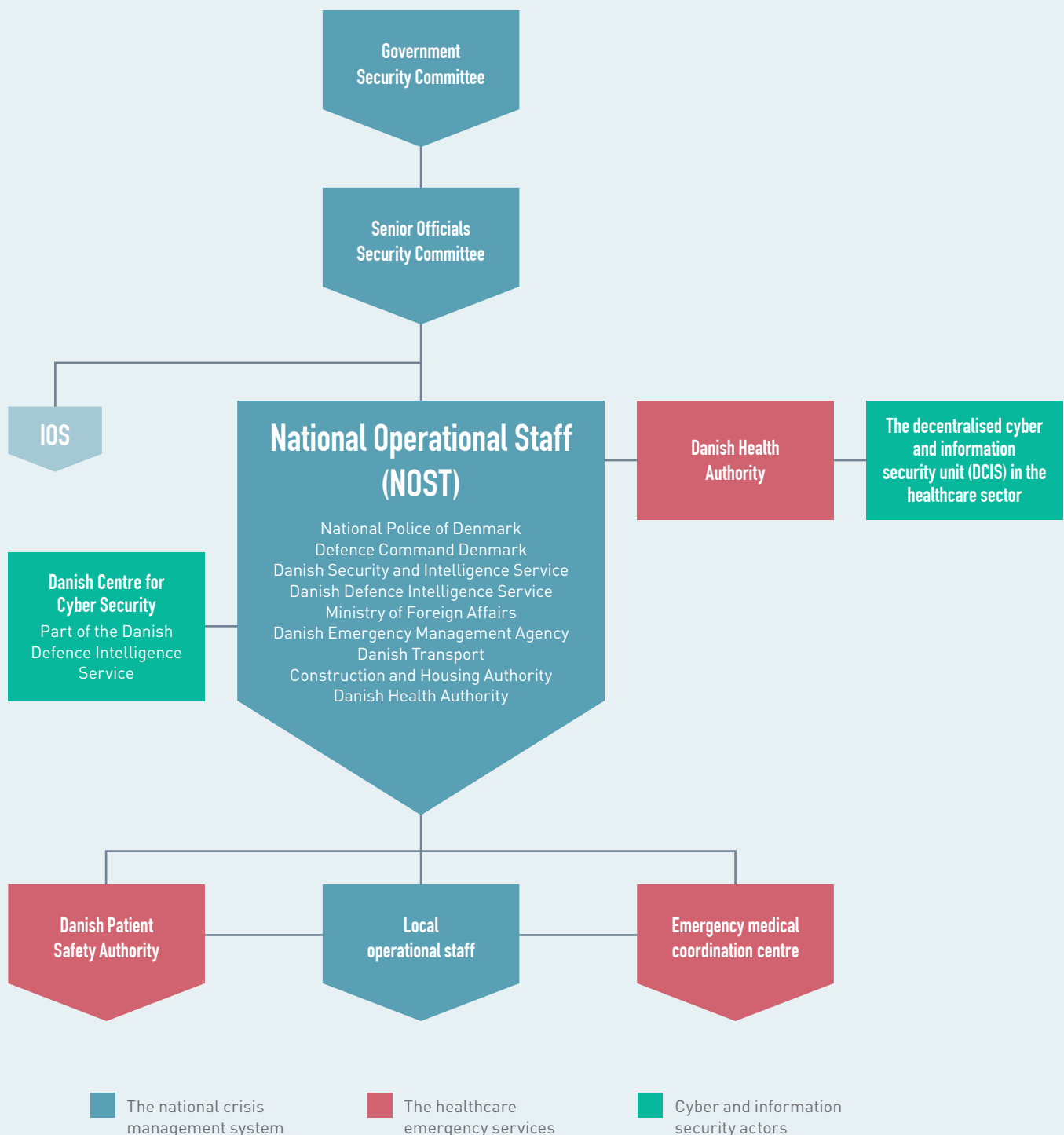
**Establishing cross-sectorial IT and cyber emergency response**

3

**Emergency response exercises for shared systems and supply chains**

FIGURE

# National crisis management and healthcare emergency services, including cyber and information security actors





## Roles and responsibilities

### Government Security Committee

The supreme security body in Denmark: The Prime Minister (chair), the Minister for Foreign Affairs, the Minister for Justice, and the Minister for Defence.

### Senior Officials Security Committee

Advises the Government Security Committee: Relevant permanent secretaries and heads of the Danish Security and Intelligence Service and the Danish Defence Intelligence Service.

### International Operational Staff (IOS)

Coordinates efforts regarding Danish citizens in the event of major incidents abroad.

### National Operational Staff (NOST)

Coordinates efforts in the event of major incidents in Denmark and ensures that information is provided to the government, the general public, and relevant authorities. NOST is made up of the National Police of Denmark, the Defence Command Denmark, the Ministry of Foreign Affairs, and a number of other authorities (see figure). Other authorities may be summoned as required.

### Local operational staff

Coordinates local efforts in the event of extraordinary incidents. The local operational staff includes the police, the local defence region, the Danish Emergency Management Agency's regional fire and rescue centre, the region's healthcare emergency services, and the municipal emergency services. The Danish Patient Safety Authority is an ad-hoc member.

### Danish Health Authority

The Danish Health Authority holds professional sector responsibility for the healthcare emergency services in Denmark. This includes providing advisory services to the Ministry of Health, municipalities, and regions with regard to the healthcare emergency health services. In the event of a specific incident, the Danish Health Authority will coordinate the effort in the healthcare sector with other sectors.

### Danish Patient Safety Authority

Advises local authorities on healthcare matters and undertakes emergency response tasks in cooperation with the Danish Health Authority.

### Emergency medical coordination centre

Heads the healthcare effort in the region in the event of a major incident. The emergency medical coordination centre is responsible for communication between the healthcare authorities and the incident site.

### Danish Centre for Cyber Security

As part of the Danish Defence Intelligence Service, the Danish Centre for Cyber Security will participate in NOST in the event of major, intersectorial cyber and information security incidents of national importance.

### The decentralised cyber and information security unit (DCIS) in the healthcare sector

In the event of a cyber and information security incident in the healthcare sector, the Danish Health Authority and DCIS will cooperate on the emergency response.

#### INITIATIVE 4.1.

### Incident response

In the event of a cyber and information security incident, the healthcare sector must be capable of quickly and securely dealing with the incident and restoring everyday operation. Therefore all actors in the sector must have relevant functions and procedures in place for responding to cyber and information security incidents in their own systems. To aid and assist this work, the DCIS will carry out an analysis in the first half of 2019 of the healthcare sector's existing contracts and functions for incident response locally, as well as for cross-sectorial incidents. The DCIS will also work with the actors in the sector to establish incident classifications as a starting point for clarifying the need for a shared function for responding to advanced incidents (forensics). The establishment of such a function will require additional agreement between healthcare-sector parties.

#### INITIATIVE 4.2.

### Establishing cross-sectorial IT and cyber emergency response

To ensure that the sector is capable of overcoming the effects of a major, cross-sectorial cyber and information security incident as quickly as possible, cross-sectorial processes for effective and coordinated incident response are needed. Thus the DCIS will in the first half of 2019 work with healthcare-sector actors to describe a model for the establishment of cross-sectorial cooperation on IT and cyber emergency response for the sector's shared systems and supply chains. This work will be based on and coordinated with the existing local IT and cyber emergency responses that have been implemented by sector actors, the general healthcare emergency response, and the national crisis management organisation.

#### INITIATIVE 4.3.

### Emergency response exercises for shared systems and supply chains

The healthcare sector must be capable of responding to cyber and information security incidents in an effective and coordinated manner. To this end, optimal cooperation in the sector's cross-sectorial IT and cyber emergency response must be tested regularly, and lessons learned should be shared and incorporated into incident responses processes at both the cross-sectorial and the local level. The cross-sectorial IT and cyber emergency response exercises must include incidents that affect cross-sectorial IT systems and IT infrastructure components that deliver IT services that are critical to the business of one or more actors in the healthcare sector. The costs of participation in these exercises will be kept within the budgets of the individual actors.

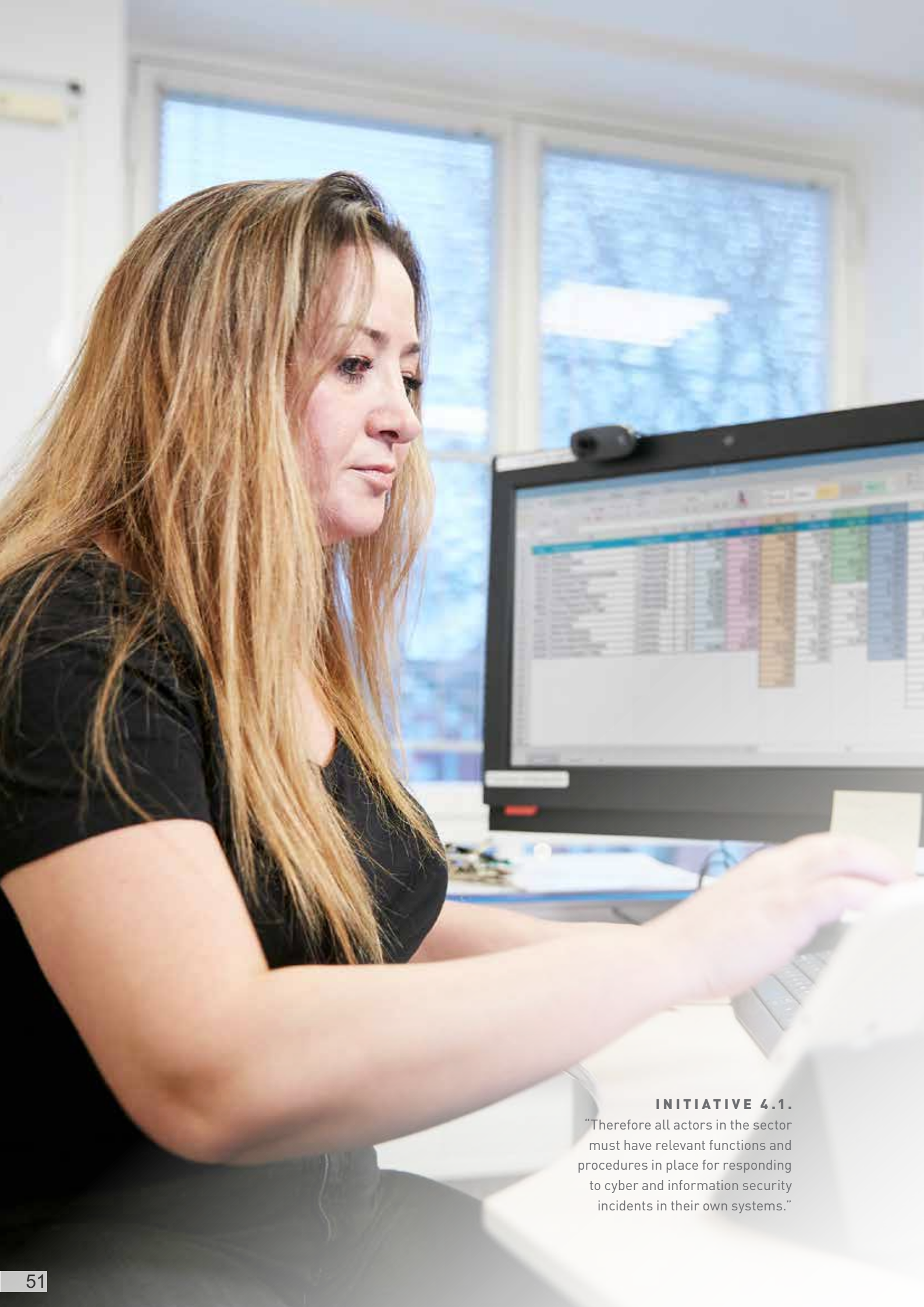
## → The deployment stages of the emergency response

Both the national emergency response and the healthcare sector's emergency response use three stages for deployment.

**Stage 1 – Information emergency response:** Activating and establishing a crisis management team is not yet considered necessary. Managers and key individuals should be vigilant. It may, for example, be necessary to undertake enhanced monitoring, notify relevant staff, and implement the procedures in the emergency response plan.

**Stage 2 – Staff emergency response:** An incident or threat may mean that crisis management teams have to be able to meet within two hours to coordinate the authorities' tasks. For instance, it may be necessary for a team of managers and staff to meet at regular intervals, but without establishing an actual crisis management team and crisis management.

**Stage 3 – Operational emergency response:** Establishment of a crisis management team that meets in order to carry out all tasks relevant to crisis management.



**INITIATIVE 4.1.**

“Therefore all actors in the sector must have relevant functions and procedures in place for responding to cyber and information security incidents in their own systems.”

# Implementation and continuous evaluation, prioritisation, and further development

This strategy sets an ambitious aim for the enhancement of the healthcare sector's joint capacity in relation to cyber and information security – and hence to future-proof the Danish healthcare service. This is a demanding task that requires regular follow-up on the implementation of the strategy and its initiatives.

This strategy has been agreed on politically between the Ministry of Health, Local Government Denmark, and Danish Regions. The follow-up on the strategy and its initiatives is overseen by the steering committee in charge of its production. This steering committee continues with some adjustments; including the expansion of the committee with a member from the Danish Health Authority's healthcare emergency response team and a member from the Danish Organisation of General Practitioners. The steering committee will meet four times a year and discuss the implementation of the strategy and report twice a year to the National Board of Health IT on the progress of this work.

**This strategy sets an ambitious aim for the enhancement of the healthcare sector's joint capacity in relation to cyber and information security – and hence to future-proof the Danish healthcare service.**

Cyber and information security is a constantly evolving field. New challenges and threats – and new opportunities as well – may arise that did not exist when the strategy was launched. Moreover, the sector is also continuously changing. Therefore the direction and the initiatives of this strategy have to be evalu-

ated each year on the basis of updated assessments of threats, vulnerabilities, and risks in the healthcare sector. To this end, an annual cycle of activities that establishes the sequence of this work is being prepared. The final assessment of whether the strategy and the existing initiatives are fully adequate

will be carried out on this basis.

A number of external reviews must be carried out annually to guarantee transparency and progress in the efforts to enhance the healthcare sector's capacity in relation to cyber and information security. Using an external party will guarantee independence from the decentralised cyber and information security unit

## → Interface between the Danish Centre for Cyber Security and healthcare-sector actors

The Danish Centre for Cyber Security primarily plays a part in relation providing advisory services and assistance to the healthcare sector. The Danish Centre for Cyber Security compiles threat assessments (both nationally and specifically for the healthcare sector), a national overview of the cyber threat situation, and disseminates notifications about current trends and relevant security incidents both to and from the healthcare sector in relation to the other sectors and to the centre's international partners. Pursuant to the sector responsibility principle, the actors in the sector are responsible for cyber and information security in the healthcare sector – including for responding to specific cyber and information security incidents. The Danish Centre for Cyber Security solely assists with actual incident response in cases in which the centre deems that an incident is of intersectorial and national relevance; and in such instances, the assistance provided by the Danish Centre for Cyber Security should be seen as a supplement to the healthcare sector's own effort.



# The DCIS is a new unit that gathers the threads, coordinates analyses and monitors progress

On 1 November 2018 a decentralised cyber and information security unit (DCIS) was created as part of the effort to strengthen the overall cyber security effort in the sector. The unit is placed in the Danish Health Data Authority and is comprised of 12-14 employees. The DCIS is tasked with gathering and coordinating cyber and information security work in the sector and will act as the sector's link to the Danish Centre for Cyber Security. In addition, the unit is, among other things, responsible for supporting the healthcare sector's implementation of the strategy for cyber and information security, including project management of the agreed analyses, coordination of notifications, preparation of guidelines and information material, facilitation of knowledge sharing, etc.

(DCIS), as the tasks performed by this unit will also be covered by the external reviews.

Finally, the decentralised cyber and information security unit (DCIS) will ensure that a method is established for gathering knowledge about the number and nature of cyber and information security incidents throughout the entire sector. This will aid to gauge the effect of the sector's overall effort. Among other things, these incident overviews will form a basis for assessing whether the cyber and information security efforts in the sector are sufficient. The fact that information on the number of attacks and security incidents must be treated confidentially must be taken into account in this regard.

A number of the strategy's activities are based on initiatives that are already being carried out by the individual actors in the sector, and therefore they are being funded and organised locally as part of the actors' own budgets. For instance, this includes the preparation of vulnerability and risk assessments, the building of awareness and skills within relevant groups of staff, etc. Similarly, the decentralised cyber and information security unit (DCIS) in the healthcare

sector will initiate activities as part of the unit's own budget, including analyses, preparing guidelines, facilitating knowledge-sharing, etc.

With this strategy the healthcare-sector parties are at the same time paving the way for a number of new collective activities that are dependent on clarifying the specific needs of the sector and the options for funding these activities. This means that the healthcare-sector parties may agree on the funding of new collective activities at a later date. Funding of new collective activities is thus included in the continuous prioritisation and adjustment of the sector's efforts – corresponding to the development in terms of new technologies, the threat pattern, and the sector itself.

This strategy defines a collective agenda for cyber and information security in the healthcare sector. Rather than providing a definitive catalogue of activities, the strategy is thus intended to be a dynamic document with guiding strategic initiatives to help the actors in the healthcare sector work together on further developing and strengthening the sector's overall cyber and information security effort.



Thank you to the North Denmark Region, Aalborg University Hospital, the home care service in the Municipality of Copenhagen, and to all the participants in photos taken for this strategy.

## The Danish healthcare sector in brief

Denmark is a small Scandinavian country in northern Europe with a population of 5.7 million and covering an area of 43,094 km<sup>2</sup>. The capital of Denmark is Copenhagen.

Healthcare in Denmark is based on two main principles:

**Free and equal access to public healthcare.** This includes general and specialised practitioner services and all-public hospital services. Private co-payment includes dentists and out-of-hospital medicines and aides.

**Universal coverage.** All residents in Denmark are entitled to public healthcare benefits in kind financed by general taxes.

The Danish healthcare sector consists of three political and administrative levels: the state (the Ministry of Health), the 5 regions, and the 98 municipalities.

The Ministry of Health is the principal healthcare authority at state level and is responsible for national healthcare policies and legislation.

The five regions in Denmark are run by elected boards and are the main service providers in the Danish healthcare system. Their responsibilities include all hospital and psychiatric treatment and parts of the primary healthcare system, including general practitioners (family doctors), privately practising specialists, and dental services for adults. As a rule, a patient must be referred to a hospital for medical examination and treatment by a general practitioner, unless it is a question of acute illness. However, the vast majority of medical cases are handled by the general practitioner without referral to specialised treatment.

The regions do not collect taxes. Instead, regional healthcare services are financed through a block grant from the state, a state activity-related subsidy, and a municipal contribution.

The 98 municipalities are the local administrative bodies with an average of approx. 57,000 inhabitants. The municipalities are responsible for a number of tasks, including social services, primary schools, and care for the elderly. In the field of healthcare, the municipalities are responsible for home nursing and homes for elderly citizens with care facilities and associated care staff, public and school healthcare, and rehabilitation.

The municipalities finance approximately 20 per cent of the total expenditure on healthcare in the regions. The payment consists of an activity-related contribution depending on their citizen's use of hospitals. The purpose of the local contributions is to encourage the municipalities to initiate efficient preventive measures for their citizens with regard to health issues.

The Danish healthcare system is characterised by extensive digitisation. All hospitals, general practitioners, and municipal healthcare providers keep electronic health records (EHR's), and common IT standards facilitate electronic communication between providers; e.g., all referrals to medical specialists and psychologist are made digitally. Overall coordination within the field of eHealth takes place in the National Board for Health IT, created in 2011 with representatives from the ministry, the regions, and the municipalities. The role of the board is to coordinate and follow the overall strategies for both digital health and cyber and information security in the healthcare sector, as well as development within eHealth, to initiate new national eHealth projects etc.

### → The Danish healthcare sector in numbers

	Denmark	OECD average
Doctors (per 1,000 inhabitants)	3.7	3.4
Number of hospital beds (per 1,000 inhabitants)	2.5	4.7
Average length of stay in hospitals (days)	5.5	7.8
Life expectancy (years)	80.8	80.6
Share of GDP spent on healthcare (percentage)	10.4	9.0

(OECD 2017)

