FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

January 2025
– 9/2024

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

The protection of health data against cyberattacks in the regions

1. Introduction

1.1. Purpose and conclusion

1. This report concerns what the regions are doing to protect hospital health data against cyberattacks. Health data can include, for example, medical records, test results, and X-ray images.

2. In May 2024, the Centre for Cyber Security assessed that the threat from cybercrime and cyber espionage against the Danish healthcare sector is very high. A successful cyberattack can disable the critical IT infrastructure of hospitals, with the consequence that patients may not receive necessary treatment. It can also result in personal health data being altered, deleted, or disclosed to unauthorized parties.

3. The Danish healthcare system is among the most digitalized in the world. Health data that was previously stored in physical paper records is now digital, including in electronic patient records, which are one of the most important tools for healthcare personnel in their daily work. Digitalization ensures that healthcare personnel have access to personal health data across the healthcare system, allowing for a coherent treatment process for patients.

However, this extensive digitalization also makes the Danish healthcare system vulnerable to cyberattacks. Health data is valuable to cybercriminals and foreign states that can gain economic or technological advantages through cyber espionage. Cybercriminals can, for example, use health data to blackmail citizens and organizations.

4. The regions are responsible for the IT systems of public hospitals, which store and provide healthcare personnel with access to health data.

Since January 2017, the regions have been required to follow the international standard for information security, ISO 27001, as part of the contract "Fællesregional Informationssikkerhedspolitik." ISO 27001 sets overarching and general requirements for working with information security. Like Rigsrevisionen's other studies on IT and cybersecurity, this study is based on ISO 27001.

Rigsrevisionen has defined 15 specific assessment criteria derived from ISO 27001 and recommendations from the Centre for Cyber Security. Some key elements include the requirement for the regions to have comprehensive knowledge of vulnerabilities in their networks and IT systems that contain health data, as well as the obligation to take necessary steps to continuously protect health data against cyberattacks. Additionally, the regions must have a contingency plan to handle the consequences of cyberattacks on IT systems containing health data.

Centre for Cyber Security
The Centre for Cyber Security is part of the Danish Defence Intelligence Service under the Danish Ministry of Defence. The Centre for Cyber Security is established to assist Danish authorities and businesses in preventing, responding to, and protecting against cyberattacks.

Critical IT infrastructure
According to the Centre for Cyber Security, critical IT infrastructure refers to digital elements that support the processing of data essential for maintaining or restoring society's vital functions.

Cybersecurity and IT security
Cybersecurity encompasses protection against digital attacks targeting data or systems via an external connection, such as through the internet.

IT security, more broadly, addresses information security for data processed within IT systems.

5. The purpose of the study is to assess whether the regions adequately protect health data in the hospital sector against cyberattacks. We answer the following questions in the report:

- Do the regions have a sufficient basis for protecting health data against cyberattacks?
- Have the regions implemented adequate measures to protect health data against cyberattacks?
- Do the regions have a contingency plan to handle the consequences of cyberattacks affecting electronic patient records?

We have examined the regions' protection of their networks and IT systems containing health data, which the regions consider critical for hospital operations. Each region has 10-20 IT systems with health data critical for hospital operations, such as electronic patient records, radiology systems, and blood test systems. In the third question, we focus on electronic patient records, which, according to the regions, are the most critical IT systems containing health data for hospital operations.

6. Rigsrevisionen initiated the study in December 2023.

Conclusion

The regions' efforts to protect health data are not entirely satisfactory. The regions have protected health data against cyberattacks, but all regions can improve their protection. The regions have generally made efforts to prevent hackers from gaining access to health data but have not done enough to limit the damage from cyberattacks in cases where hackers have succeeded in accessing health data. The consequence is that hackers can more easily spread their attacks and potentially disrupt larger parts of the hospital sector.

The regions' basis for protecting health data against cyberattacks varies

All regions have policies and guidelines on how to protect health data. All regions also have an overview of their IT systems containing health data and conduct vulnerability management. However, two regions have yet to assess how critical their IT systems are for hospital management, and two regions lack a consolidated follow-up on vulnerability management at the management level. Additionally, one region has not developed risk assessments and action plans for health data security.

The regions have implemented several relevant measures to protect health data against cyberattacks but have not done enough to limit the damage from successful cyberattacks

All regions have generally implemented measures to prevent hackers from gaining access to their networks containing health data. These measures include using secure passwords and applying security updates to network equipment. However, the study shows that the regions have not done enough to prevent the spread of successful cyberattacks. For example, the regions have only to a limited extent worked on segmenting their critical IT systems with health data. Furthermore, several regions have not adequately updated the security of computers and mobile devices with access to health data.

The regions' contingency plans for electronic patient records vary

Two regions have a contingency plan to handle the consequences of cyberattacks affecting electronic patient records. The other three regions have various deficiencies in their contingency planning. The study shows, for example, that two regions have not regularly tested their contingency plans and do not have documented procedures for restoring electronic patient records. All regions have taken backups of electronic patient records, but two regions have not sufficiently tested whether their backup can be used to restore electronic patient records in case of a system failure.

All regions have improved their security during the study period based on Rigsrevisionen's findings and have stated that they will continue to work on enhancing their protection of health data against cyberattacks.