RIKS REVISIONEN

Date: 2024-03-26
Reference number: 2022/1031
RiR 2024:6

Information security in health and social care

–central government support and supervision

Summary

Health and social care providers handle large amounts of sensitive personal data digitally in many different IT systems and are responsible for the information security of this personal data. This means, for example, that personal data must be processed in a way that ensures sufficient protection. The central governments task it to support and supervise health and social care providers' work with information security to ensure that it is conducted systematically and risk-based according to regulatory requirements. Several government agencies are tasked with steering, supporting, monitoring and supervising the information security of health and social care providers. The audit of the Swedish National Audit Office ("the Swedish NAO") shows that the efforts of the central government are not effective. The measures taken by the government and agencies have not been sufficient to strengthen the information security work of health and social care providers and thus raise their information security level. A central deficiency is that the agencies' support is not adapted to their needs and that supervision is limited.

Support not sufficiently adapted to the needs of health and social care

The support of the Swedish Authority for Privacy Protection (IMY), the Swedish Civil Contingencies Agency (MSB) and the National Board of Health and Welfare is not

Riksrevisionen (Swedish National Audit Office)
www.riksrevisionen.se
S:t Eriksgatan 117
Box 6181, 102 33 Stockholm, Sweden
+46-8-5171 40 00

effective in strengthening information security in health and social care. The agencies' support is general and mainly provides basic guidance when a provider is to build up systematic and risk-based information security work. However, the support is not sufficiently adapted to the needs of health and social care providers so that it can be implemented in their information security work in practice. This concerns, for example, issues relating to security measures in trade-offs between information security, privacy and patient safety, which requires support in interpreting legislation. To a great extent, the agencies have chosen not to take legal positions on how the requirements in the regulations applying to health and social care can be interpreted, which makes it difficult for health and social care providers to understand what is expected of them.

It is small municipalities in particular that have limited resources and difficulty in recruiting staff with the expertise required to systematically work with and ensure adequate information security. Deficient support from government agencies can therefore lead to varying levels of protection for personal data in different parts of the country. Neither MSB, IMY, nor the National Board of Health and Welfare consider themselves to be responsible for meeting needs within health and social care for specific support. The agencies also work in silos and have not cooperated or coordinated their efforts in designing their support. Furthermore, the audit shows that the support of the Swedish Civil Contingencies Agency and the Swedish Authority for Privacy Protection in transpired IT incidents is limited. Health and social care providers that have suffered cyberattacks, for example, rarely receive operational support from the Swedish Civil Contingencies Agency to alleviate the effects of the incident.

Supervision is limited and it is unclear whether it targets the areas that would benefit most

The supervision of the Health and Social Care Inspectorate (IVO) and the Swedish Authority for Privacy Protection of the information security of health and social care providers does not effectively contribute to strengthening the protection of personal data. Since 2018, when the General Data Protection Regulation and the Information Security for Essential and Digital Services Act (the NIS Act) came into force, the Swedish Authority for Privacy Protection and the Health and Social Care Inspectorate have conducted few supervisory cases of healthcare providers and none at all of social care providers. Additionally, their supervision has rarely covered all aspects of an organisation's information security. Furthermore, IVO has conducted limited supervision pursuant the NIS Act, which means that the agency has not fully examined the actual security of healthcare providers' information systems and networks in which personal data is processed. All in all, this means that central government control of the information security of health and social care providers and compliance with administrative requirements is not effective. As a result, the operations covered by the supervision do not receive sufficient guidance on how to

improve their information security work. Also, the supervision is only partly risk-based, which makes it difficult to assess whether it targets activities where it would have the greatest benefit. IMY and IVO have not followed up on supervisory decisions, and it is therefore unclear whether the audited activities have remedied the deficiencies identified in their supervision.

The Government has not ensured cohesive management

The Government has taken few measures to strengthen the information security work of health and social care providers. The government has not clearly established the division of responsibilities and duties between IMY, MSB and the National Board of Health and Welfare in terms of designing support that meets the needs of health and social care. Neither has the government ensured that the agencies coordinate their work so as to design support effectively. Although social care providers often process personal data as sensitive as that processed within healthcare, the Government has not sufficiently acted for social care providers to be subject to the same clear requirements for security measures and systematic information security work as healthcare providers, except for in certain allocations of access rights and in controls of access rights.

Recommendations

To the Government

- Clarify the responsibility of the National Board of Health and Welfare in terms of developing specifical support for the information security work of health and social care that is adapted to the operations. The support should be designed based on the needs of health and social care providers and in consultation with relevant authorities. The support may include, for example:
    - identifying sector-specific information security risks and vulnerabilities.
    - providing examples of appropriate organisational and technical security measures for information security.
    - providing support and guidance on how provisions on the protection of personal data should be interpreted in general cases.
- Investigate how social care providers can be fully covered by provisions governing the protection of personal data equivalent to those for healthcare providers.
- Ensure that social care providers and small-scale healthcare providers that are not covered by the NIS Act are subject to requirements to conduct systematic and risk-based information security work.

To the Health and Social Care Inspectorate

- Conduct supervision that examines whether healthcare providers actually meet all of the requirements of the NIS Act concerning security in networks and information systems.
- Develop the work with risk analyses so that supervision is focused to a greater extent on areas where information security deficiencies are greatest.
- Develop follow-up of supervisory decisions to ensure that supervision has the intended effect.

To the Swedish Authority for Privacy Protection

- Improve efficiency in processing complaint and supervision cases, thus freeing up resources to conduct more risk-based supervision.
- Develop the work with risk analyses so that supervision is focused to a greater extent on areas where information security deficiencies are greatest.
- Develop follow-up of supervisory decisions to ensure that supervision has the intended effect.