FOLKETINGET
RIGSREVISIONEN

December 2026

Rigsrevisionens notat om beretning om

regionernes beskyttelse af sundhedsdata mod cyberangreb

Opfølgning i sagen om regionernes beskyttelse af sundhedsdata mod cyberangreb (beretning nr. 9/2024)

24. november 2026

RN C122/26

I. Baggrund og konklusion

1. Rigsrevisionen følger i dette notat op på sagen om regionernes beskyttelse af sundhedsdata mod cyberangreb, som blev indledt med en beretning i 2025. Opfølgningen sker med henblik på at vurdere, om de initiativer, som den daværende indenrigs- og sundhedsminister og regionerne stillede Statsrevisorerne i udsigt i lyset af Statsrevisorernes bemærkninger og Rigsrevisionens beretning, er gennemført. Vi har tidligere behandlet sagen i notat til Statsrevisorerne af 23. juni 2025.

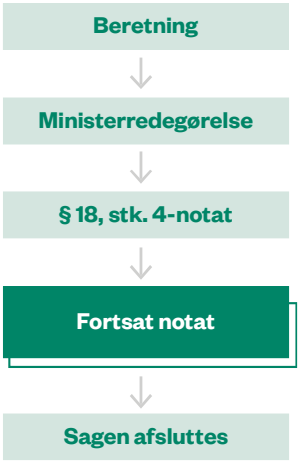
2. Formålet med beretningen var at vurdere, om regionerne i tilstrækkeligt omfang beskytter sundhedsdata i hospitalsvæsenet mod cyberangreb.

3. Da Statsrevisorerne behandlede beretningen, fandt de, at regionernes beskyttelse af sundhedsdata ikke var helt tilfredsstillende. Dermed var der risiko for, at følsomme og fortrolige sundhedsdata kom i hænderne på uvedkommende eller ikke var pålidelige og tilgængelige, når der er brug for dem. Statsrevisorerne konstaterede, at regionerne generelt havde gjort en indsats for at forhindre, at hackere opnår adgang til sundhedsdata. Alle regionerne havde desuden forbedret deres cybersikkerhed i undersøgelsesperioden.

Konklusion

Rigsrevisionens opfølgning viser, at Region Syddanmark, Region Hovedstaden og Region Sjælland har styrket deres grundlag for at beskytte sundhedsdata mod cyberangreb. Region Hovedstaden er dog ikke helt i mål med at vurdere, hvor kritiske deres it-systemer med sundhedsdata er for hospitalsdriften, så de kan prioritere de vigtigste it-systemer først i en krisesituation. Ledelserne i Region Sjælland og Region Syddanmark mangler at sikre, at der også bliver fulgt op på de mindre kritiske sårbarheder, som regionerne finder i forbindelse med sårbarhedsskanninger.

Sagsforløb for en større undersøgelse



Du kan læse mere om forløbet og de enkelte step på www.rigsrevisionen.dk

Rigsrevisionens opfølgning viser videre, at Region Nordjylland nu har taget tilstrækkelige tiltag til at beskytte sundhedsdata mod cyberangreb på de undersøgte områder. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes for Region Nordjylland. De øvrige regioner har fortsat mangler i deres tiltag til at beskytte sundhedsdata mod cyberangreb. Fx mangler tre regioner fortsat at segmentere alle it-systemer med sundhedsdata, der er kritiske for hospitalsdriften.

Endelig viser opfølgningen, at Region Syddanmark og Region Nordjylland har gennemført de planlagte initiativer til at sikre beredskabet. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes for disse to regioner. Region Midtjylland mangler at teste dele af deres reetableringsplan regelmæssigt.

Rigsrevisionen vil fortsat følge udviklingen og orientere Statsrevisorerne om:

- Region Syddanmarks, Region Hovedstadens og Region Sjællands initiativer til at styrke grundlaget for at beskytte sundhedsdata mod cyberangreb
- Region Syddanmarks, Region Midtjyllands, Region Sjællands og Region Hovedstadens tiltag til at beskytte sundhedsdata mod cyberangreb
- Region Midtjyllands arbejde med at teste deres reetableringsplan.

II. Status på sagen

4. På baggrund af beretningen og Statsrevisorernes bemærkninger har vi fulgt op på følgende punkter:

Et opfølgningspunkt afsluttes, når Statsrevisorerne på baggrund af indstilling fra Rigsrevisionen vurderer, at myndighedernes initiativer er tilfredsstillende.

Opfølgningspunkt	Status
1. Region Syddanmarks, Region Hovedstadens og Region Sjællands initiativer til at styrke grundlaget for at beskytte sundhedsdata mod cyberangreb.	Behandles i dette notat og følges fortsat for alle tre regioner.
2. Regionernes tiltag til at beskytte sundhedsdata mod cyberangreb.	Region Nordjylland behandles og afsluttes i dette notat. Region Syddanmark, Region Midtjylland, Region Sjælland og Region Hovedstaden behandles i dette notat og følges fortsat.
3. Region Syddanmarks, Region Midtjyllands og Region Nordjyllands initiativer til at sikre et fuldstændigt beredskab.	Region Syddanmark og Region Nordjylland behandles og afsluttes i dette notat. Region Midtjylland behandles i dette notat. Vi vil fortsat følge regionens arbejde med at teste deres reetableringsplan.

III. Regionernes initiativer

5. Vi gennemgår i det følgende regionernes initiativer i forhold til opfølgningspunkterne.

6. Opfølgningen er baseret på dokument- og systemgennemgang.

Regionernes grundlag for at beskytte sundhedsdata mod cyberangreb

Region Syddanmark, Region Hovedstaden og Region Sjælland har styrket deres grundlag for at beskytte sundhedsdata mod cyberangreb. Region Hovedstaden er dog ikke helt i mål med at vurdere, hvor kritiske deres it-systemer med sundhedsdata er for hospitalsdriften. Ledelserne i Region Sjælland og Region Syddanmark mangler at sikre, at der bliver fulgt op på de mindre kritiske sårbarheder, som regionerne finder i forbindelse med sårbarhedsskanninger. Rigsrevisionen vil fortsat følge Region Syddanmarks, Region Hovedstadens og Region Sjællands initiativer til at styrke grundlaget for at beskytte sundhedsdata mod cyberangreb.

7. Statsrevisorerne bemærkede, at alle regionerne havde politikker og retningslinjer for, hvordan de skulle beskytte sundhedsdata, men Region Syddanmark og Region Hovedstaden manglede at vurdere, hvor kritiske de enkelte it-systemer var for hospitalsdriften. Denne vurdering er nødvendig, for at regionerne kan prioritere de vigtigste it-systemer først i en krisesituation. Ledelserne i Region Sjælland og Region Syddanmark havde ikke sikret, at der blev fulgt op på alle resultaterne af deres sårbarhedsskanninger, og Region Sjælland manglede desuden at udarbejde risikovurderinger og handleplaner for sikkerheden omkring sundhedsdata.

8. Vores opfølgning viser, at Region Hovedstaden, Region Sjælland og Region Syddanmark har styrket deres grundlag for at beskytte sundhedsdata mod cyberangreb. Status for de udestående punkter fremgår af tabel 1.

Tabel 1

Regionernes grundlag for at beskytte sundhedsdata mod cyberangreb i 2026

	Region Hovedstaden	Region Sjælland	Region Syddanmark
Har regionen et overblik over, hvor kritiske deres it-systemer med sundhedsdata er for hospitalsdriften?	●	●	●
Har ledelsen i regionen sikret, at der bliver fulgt op på alle resultaterne af sårbarhedsskanninger?	●	●	●
Har regionen opdaterede og ledelsesgodkendte risikovurderinger og handleplaner?	●	●	●

● Ja ● Delvist ○ Nej ● Opfyldt i 2025 og følges ikke længere

Note: Når vurderingskriteriet er opfyldt, markerer vi det med grønt. Et vurderingskriterie er delvist opfyldt og markeres med gult, hvis vi vurderer, at en delmængde af de nødvendige elementer er til stede. Et vurderingskriterie er ikke opfyldt og markeres med rødt, hvis ingen af de nødvendige elementer er til stede.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Tabel 1 viser, at Region Syddanmark nu har vurderet, hvor kritiske alle deres it-systemer med sundhedsdata er for hospitalsdriften. Region Hovedstaden er i gang med at vurdere, hvor kritiske deres it-systemer med sundhedsdata er, men har ikke fremsendt dokumentation for, at de er i mål med arbejdet.

Tabel 1 viser også, at ledelserne i Region Sjælland og Region Syddanmark delvist har sikret, at der bliver fulgt op på alle resultaterne af sårbarhedsskanningerne. I begge regioner følger ledelsen op på, at kritiske sårbarheder bliver håndteret, men regionerne mangler stadig at sikre, at også de mindre kritiske sårbarheder fra sårbarhedsskanningerne bliver håndteret.

Endelig viser tabel 1, at Region Sjælland nu har udarbejdet risikovurderinger og handleplaner for sikkerheden omkring deres it-systemer med adgang til sundhedsdata.

Regionernes tiltag til at beskytte sundhedsdata mod cyberangreb

Rigsrevisionens opfølgning viser, at Region Nordjylland nu har taget tilstrækkelige tiltag til at beskytte sundhedsdata mod cyberangreb på de undersøgte områder. Rigsrevisionen vurderer på den baggrund, at denne del af sagen kan afsluttes for Region Nordjylland.

De øvrige regioner har fortsat mangler i deres tiltag til at beskytte sundhedsdata mod cyberangreb. Fx mangler tre regioner fortsat at segmentere alle it-systemer med sundhedsdata, der er kritiske for hospitalsdriften. Rigsrevisionen vil fortsat følge Region Syddanmarks, Region Midtjyllands, Region Sjællands og Region Hovedstadens tiltag til at beskytte sundhedsdata mod cyberangreb.

9. Statsrevisorerne bemærkede, at alle regionerne generelt havde iværksat tiltag, der skulle forhindre, at hackere kan opnå adgang til regionernes netværk med sundhedsdata. Region Hovedstaden anvendte dog ikke multifaktorlogin og havde ikke segmenteret netværket. Hvis it-systemerne ikke er inddelt i segmenter, er der risiko for, at fx et cyberangreb spreder sig fra ét it-system til et andet.

Det fremgik af beretningen, at de andre regioner heller ikke havde foretaget en tilstrækkelig segmentering af de it-systemer med sundhedsdata, som de selv vurderede som kritiske for hospitalsdriften.

Det fremgik desuden, at regionerne også på andre områder ikke havde en tilstrækkelig beskyttelse af sundhedsdata mod cyberangreb. Region Sjælland havde kun delvist en hensigtsmæssig brug af firewalls, og Region Midtjylland havde kun delvist implementeret en systematisk logning og overvågning af netværkstrafikken. Flere af regionerne havde også pc'er, mobile enheder eller servere, der ikke var tilstrækkeligt sikkerhedsopdaterede.

10. Vores opfølgning viser, at regionerne generelt har arbejdet på at sikkerhedsopdatere deres servere. Fire regioner har dog fortsat mangler i deres tiltag til at beskytte sundhedsdata mod cyberangreb. Status for de udestående punkter fremgår af tabel 2.

Multifaktorlogin
Multifaktorlogin betyder, at en medarbejder skal bruge to eller flere faktorer for at opnå adgang til et it-system. En faktor er fx et password, en kode sendt til en mobil enhed via en app eller biometriske data som fingeraftryk eller ansigtsgenkendelse.

Mobile enheder
Regionerne anvender i nogle tilfælde mobiltelefoner, tablets eller håndskannere med adgang til sundhedsdata.

Tabel 2
Regionernes tiltag til at beskytte sundhedsdata mod cyberangreb i 2026

	Region Hovedstaden	Region Sjælland	Region Syddanmark	Region Midtjylland	Region Nordjylland
Bruger regionen multifaktorlogin på netværksudstyret?	●	●	●	●	●
Har regionen segmenteret netværket?	●	●	●	●	●
Har regionen en hensigtsmæssig brug af firewalls?	●	●	●	●	●
Har regionen implementeret systematisk logning og overvågning af netværkstrafikken?	●	●	●	●	●
Har regionen sikret, at mobile enheder og pc'er med adgang til sundhedsdata er sikkerhedsopdaterede?	●	●	●	●	●

● Ja ● Delvist ○ Nej ● Opfyldt i 2025 og følges ikke længere

Note: Se forklaring af farvemarkeringer i tabel 1. Resultaterne vedrørende regionernes sikkerhedsopdatering af servere er ikke afrapporteret i tabel 2, da én af regionerne vurderer, at oplysningerne er fortrolige efter forvaltningsloven.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Tabel 2 viser, at Region Hovedstaden nu bruger multifaktorlogin på deres netværksudstyr.

Tabel 2 viser også, at Region Nordjylland og Region Sjælland har segmenteret de it-systemer med sundhedsdata, der er kritiske for hospitalsdriften. De øvrige regioner er nået længere med deres segmentering siden beretningen, men de er endnu ikke i mål.

Region Sjælland har påbegyndt et arbejde med at sikre en regelmæssig gennemgang af regionens firewalls, men regionen er endnu ikke i mål med gennemgangen.

Region Midtjylland har nu implementeret en systematisk logning og overvågning af netværkstrafikken.

Endelig viser tabel 2, at Region Nordjylland nu har sikkerhedsopdateret alle deres pc'er og mobile enheder, der giver adgang til sundhedsdata. Region Hovedstaden og Region Sjælland har fortsat mobile enheder med adgang til sundhedsdata, der ikke er tilstrækkeligt sikkerhedsopdaterede.

Regionernes initiativer til at sikre et fuldstændigt beredskab

Rigsrevisionens opfølgning viser, at Region Syddanmark og Region Nordjylland har gennemført de planlagte initiativer til at sikre beredskabet. Region Midtjylland mangler fortsat at teste dele af deres reetableringsplan regelmæssigt. Rigsrevisionen vil derfor fortsat følge Region Midtjyllands arbejde hermed.

11. Statsrevisorerne bemærkede, at alle regionerne havde et beredskab til at håndtere konsekvenserne af cyberangreb, men at dele af beredskabet var mangelfuldt i Region Midtjylland, Region Nordjylland og Region Syddanmark. Alle regionerne havde beredskabsplaner til at håndtere cyberangreb, der rammer de elektroniske patientjournaler, men Region Midtjylland og Region Syddanmark havde ikke testet deres beredskabsplaner regelmæssigt, og de to regioner manglede reetableringsplaner, der udgør en vigtig del af regionernes beredskabsplaner. Planerne sikrer, at regionerne har en plan for, hvordan patientjournalerne kan genskabes efter nedbrud. Endelig havde regionerne taget backup af de elektroniske patientjournaler, men Region Nordjylland og Region Syddanmark havde ikke i tilstrækkeligt omfang testet, om deres backup kunne bruges til at reetablere de elektroniske patientjournaler ved nedbrud.

12. Tabel 3 viser status på regionernes initiativer til at sikre et fuldstændigt beredskab.

Tabel 3
Regionernes initiativer til at sikre et fuldstændigt beredskab

	Region Syddanmark	Region Midtjylland	Region Nordjylland
Har regionen en opdateret beredskabsplan for de elektroniske patientjournaler, herunder en krisestyringsplan, nødplan og reetableringsplan, som de tester regelmæssigt?	●	●	●
Har regionen testet, at deres backup kan bruges til at reetablere de elektroniske patientjournaler?	●	●	●

● Ja ● Delvist ○ Nej ● Opfyldt i 2025 og følges ikke længere

Note: Se forklaring af farvemarkeringer i tabel 1.

Kilde: Rigsrevisionen på baggrund af dokumentation fra regionerne.

Tabel 3 viser, at Region Syddanmark nu tester deres beredskabsplan herunder deres reetableringsplan regelmæssigt.

Region Midtjylland har udarbejdet en reetableringsplan, men mangler at teste den fuldt ud. Region Midtjylland har oplyst, at det er dyrt at gennemføre fuld test af reetableringsplanen. Det anerkender Rigsrevisionen. Set i lyset af at den elektroniske patientjournal er samfundskritisk, er det dog vigtigt, at regionen tester alle væsentlige dele af reetableringsplanen, for at sikre, at patientjournalen kan reetableres ved nedbrud.

Opfølgningen viser desuden, at Region Syddanmark og Region Nordjylland nu tester, at deres backup kan bruges til at gendanne de elektroniske patientjournaler ved nedbrud.

13. Hele sagen kan følges på www.rigsrevisionen.dk og på www.ft.dk/Statsrevisorerne.

14. Bilag 1 viser Folketingets behandling af beretningen.

Birgitte Hansen
rigsrevisor

Bilag 1. Folketingets behandling af beretningen

Beretning (nr.), dato for Statsrevisorernes mødebehandling og ministerredegørelse(r)	Behandlet i udvalg	Gennemgang ved Statsrevisorerne og Rigsrevisionen	Udvalgsspørgsmål (nr.)	Indkaldt til samråd	Statsrevisorerne har holdt møde med ministeren	§ 20-spørgsmål
Regionernes beskyttelse af sundhedsdata mod cyberangreb (nr. 9/2024) 20-01-2025 **Ministerredegørelse:** Indenrigs- og sundhedsministeren: 23-05-2025	Finansudvalget: 23-01-2025 Sundhedsudvalget: 28-01-2025 10-06-2025		Indenrigs- og sundhedsministeren: 30-01-2025 (253) 30-01-2025 (254)			