Hacking Healthcare - Weekly Blog

Hacking Healthcare	**TLP:WHITE**	**Alert Id: dcef4428**	**2025-01-24 18:58:19**

This week, Health-ISAC®'s Hacking Healthcare® examines the new EU Action Plan designed to improve the cybersecurity of hospitals and healthcare providers. Join us as we provide an overview of what's in the Action Plan before we analyze the effort in more depth in the Action & Analysis section.

Welcome back to Hacking Healthcare®.

Join Us for the Monthly Threat Briefing

But first, as a reminder, next Tuesday and Wednesday is the Health-ISAC's monthly threat briefing. Come join your fellow Health-ISAC members as Health-ISAC staff and partner organizations provide an overview of the threat landscape. Presentations include an assessment of emerging malware, APT trends, legal and regulatory issues, physical security concerns, and more. We encourage all Health-ISAC members to take advantage of this service.

European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers

Back in August of last year, *Hacking Healthcare* reviewed what Ursula von der Leyen, then recently re-elected to the position of President of the European Commission, had outlined as policy priorities for the upcoming European Commission session.[i] Included in her 31-page policy position paper, *Europe's Choice: Political Guidelines for the Next European Commission 2024-2029,*[ii] was a proposal for "a European action plan on the cybersecurity of hospitals and healthcare providers in the first 100 days of the mandate."[iii]

On January 15, von der Leyen delivered on that proposal with the publication of the *European Action Plan on the Cybersecurity of Hospitals and Healthcare Providers*.[iv]

What is the Action Plan?

At a high level, the Action Plan proposes EU-level coordination and measures from the Commission, ENISA, and member states to improve the cybersecurity of hospitals and healthcare providers. Lines of effort will include providing tailored guidance, tools, services, and training to hospitals and healthcare providers, and these actions will fall broadly into four prioritization buckets: Prevent, Detect, Respond and Recover, and Deter.

What is the justification for the Action Plan?

The European Commission cited numerous justifications for the Action Plan that included an increase in frequency and sophistication of cyber threat activity against the health sector; the criticality of healthcare provider services and the need to mitigate patient harm; concern around the erosion of public trust resulting from attacks against the health sector; a desire to improve security and resiliency during a period of digital transformation and expanding attack surfaces; and the potential to complement flagship policies like the European Health Data Space.

Who would the Action Plan apply to?

The Action Plan's scope is broadly defined as "predominantly [focusing] on the cybersecurity of hospitals and healthcare providers."[v] However, it also acknowledges that it should take into consideration the broader ecosystem and supply chain.

What does the Action Plan Propose?

The Action Plan includes a long list of proposed actions that would need to be carried out by the European Commission itself, the European Cybersecurity Agency ENISA, European member state governments, and by various elements of the private sector. Some of the more significant proposals include:

- ENISA – The creation of a dedicated European Cybersecurity Support Centre for hospitals and healthcare providers.
- ENISA – The creation of a European known exploited vulnerabilities (KEV) catalogue for medical devices, electronic health record systems and providers of ICT equipment and software in health.
- ENISA – The development of cyber incident response playbooks tailored for healthcare.
- EU Commission – The development of pilot programs to develop best practices for cyber hygiene and security risk assessment, as well as addressing the need for continuous cybersecurity monitoring, threat intelligence, and incident response.
- Member States – Would be encouraged to facilitate resource sharing among health providers, potentially through joint procurement or pooled resources to increase bargaining power with cybersecurity service providers.
- Member States – Would be encouraged to set non-binding funding benchmarks for healthcare sector entities and monitor funding targets.
- Industry – Cybersecurity companies, foundations, educational institutions, and industry stakeholders would be encouraged to pledge actions to address the challenges in the sector (e.g. Enhancing cybersecurity training, driving awareness activities, providing managed security services at reduced cost, and sharing threat intel with ENISA).

There are far too many proposed actions to cover them all here, but the Annex of the Action Plan contains a comprehensive overview sorted by responsible entity.

What comes next?

The European Commission is expected to launch public consultations soon. Alongside the consultations, the European Commission has said that discussions will continue with member states and "relevant networks" to "collect more insights." The results of the feedback is intended to inform further recommendations and revisions to the Action Plan by the end of the year.

Action & Analysis
Available with Health-ISAC Membership

[i] https://health-isac.org/health-isac-hacking-healthcare-8-9-2024/

[ii]https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

[iii]https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

[iv]https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers

[v] Is defined in-text as “any natural or legal person—or any other entity—legally providing healthcare on the territory of a Member State”

Reference(s): Europa Analytics, Europa Analytics, health-isac
Report Source(s): Health-ISAC
Release Date: Jan 25, 2025 (UTC)

Tags: Hacking Healthcare, ENISA, EU, Europe, European Commission
TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.
For Questions and/or Comments:
Please email us at contact@h-isac.org
Conferences, Webinars, and Summits:
https://h-isac.org/events/
Hacking Healthcare:
Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Councils efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Councils Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISACs annual Hobby Exercise and provides legal and regulatory updates for the Health-ISACs monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Threat Intelligence Portal:
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).
For Questions or Comments:
Please email us at toc@h-isac.org