HACKING HEALTHCARE

Hacking Healthcare - Weekly Blog

TLP:WHITE

Jun 19, 2025

This week, Health-ISAC®'s Hacking Healthcare® looks at how the European Commission continues to support its action plan to improve the cybersecurity of hospitals and healthcare providers directly and indirectly with new funding opportunities totaling nearly €150 million. Join us as we investigate what the European Commission wants to achieve and how it might affect Health-ISAC members.

Welcome back to Hacking Healthcare®.

Monthly Threat Brief

First, as a reminder, next Tuesday and Wednesday are 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.

E.U. Earmarks Additional Funds to Improve EU Cybersecurity—Healthcare Included

The European Union has been very active over the past few years in introducing new or revising existing regulations and directives, developing new initiatives, and dedicating funding with the intent of improving the security and resiliency of the European cybersecurity ecosystem. Last week, the European

Commission announced another step to bolster these efforts with two calls for proposals totaling €145.5 million "to boost European cybersecurity, including for hospitals and healthcare providers."[i] Let's dig into this new development to assess what it may mean for health sector entities in the EU and how it ties into ongoing efforts like the action plan on cybersecurity in hospitals and healthcare.[ii]

What Are the Proposals?

The first proposal is under the Digital Europe Programme (DEP). Established in 2021, the DEP is a "funding programme focused on bringing digital technology to businesses, citizens and public administrations" whose budget runs into the billions.[iii] From this program, €30 million will be made available to "enhance the cybersecurity of hospitals and healthcare providers, helping them detect, monitor, and respond to cyber threats, particularly ransomware."[iv]

The second proposal is under the Horizon Europe Programme. This funding program "strengthens the impact of research and innovation in developing, supporting and implementing EU policies while tackling global challenges," and "supports creating and better dispersing of excellent knowledge and technologies."[v] Funding for the years 2021–2027 amounted to €93.5 billion, of which €90.5 million is being made available for this opportunity to "support the use and development of generative AI for cybersecurity applications, new advanced tools and processes for operational cybersecurity, and privacy-enhancing technologies as well as post-quantum cryptography."[vi]

How Will This Support the Health Sector Specifically?

The EU Funding and Tenders Portal webpage for the first proposal provides greater detail on what it is hoped this funding opportunity will create.[vii]

Titled *Dedicated Action to Reinforcing Hospitals and Healthcare Providers*, this funding opportunity is specifically seeking to achieve the following outcomes:[viii]

- Mapping of common cybersecurity needs of hospitals and healthcare providers.
- Guidelines for healthcare providers to assess their current state of cybersecurity protection and relevant needs.
- Technical cybersecurity plans to enhance preparedness and cyber resilience: improved detection and response capabilities for healthcare institutions minimising the impact of cyberattacks, particularly for ransomware. This also includes dedicated training courses to staff.

- Pilot cybersecurity demo installations at partner hospitals and healthcare provider sites to ensure hospitals and healthcare providers can maintain operational continuity in the face of cybersecurity incidents. This should be monitored through specific KPIs.
- Wide dissemination campaigns to help scale up preparedness of hospitals and healthcare providers in Europe.

According to the proposal, all of these objectives will generally "contribute to the EU action plan on cybersecurity in hospitals and healthcare," and the various pilot projects that are envisioned making up this proposal are expected to also support healthcare institutions complying with the NIS 2 Directive.

Complete details of this proposal, including the criteria for submissions, due dates, and key performance indicators, can be found in the 43-page full proposal from the European Cybersecurity Competence Centre (ECCC).[ix]

Action & Analysis
Available with Health-ISAC Membership

[i] https://digital-strategy.ec.europa.eu/en/news/eu-allocates-eu1455-million-boost-european-cybersecurity-including-hospitals-and-healthcare
[ii] https://digital-strategy.ec.europa.eu/en/factpages/cybersecurity-hospitals-and-healthcare-providers
[iii] https://digital-strategy.ec.europa.eu/en/activities/digital-programme
[iv] https://digital-strategy.ec.europa.eu/en/news/eu-allocates-eu1455-million-boost-european-cybersecurity-including-hospitals-and-healthcare
[v] https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en
[vi] https://digital-strategy.ec.europa.eu/en/news/eu-allocates-eu1455-million-boost-european-cybersecurity-including-hospitals-and-healthcare
[vii] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH?isExactMatch=true&status=31094501,31094502,31094503&programmePeriod=2021%20-%202027&frameworkProgramme=43152860&callIdentifier=DIGITAL-ECCC-2025-DEPLOY-CYBER-08&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate
[viii] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH?isExactMatch=true&status=31094501,31094502,31094503&programmePeriod=2021%20-

%202027&frameworkProgramme=43152860&callIdentifier=DIGITAL-ECCC-2025-DEPLOY-CYBER-08&order=DESC&pageNumber=1&pageSize=50&sortBy=startDate
[ix] https://cybersecurity-centre.europa.eu/document/download/da2e1929-9320-4ae7-97e6-4c3e2ae7de3f_en?filename=DIGITAL-ECCC-2024-DEPLOY-CYBER-08.pdf
[x] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers
[xi] https://digital-strategy.ec.europa.eu/en/factpages/cybersecurity-hospitals-and-healthcare-providers

Reference(s)	europa, europa, europa, europa, europa, europa, europa
Report Source(s)	Health-ISAC

Release Date
Jun 19, 2025 (UTC)

Alert ID 1e4c0af0

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback
was this helpful? | |

Tags Action Plan, Funding, Hacking Healthcare, European Commission

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

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.

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories
For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

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

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.