Hacking Heathcare - Weekly Blog

Hacking Healthcare	TLP:WHITE	Alert Id: 4d72d6de	2025-03-21 17:25:09

This week, Health-ISAC®'s Hacking Healthcare® examines a new cyber incident reporting regime coming into force in Switzerland. Join us as we assess how the new law might affect health sector entities, how it interacts and compares to existing reporting regimes in Europe, and how it fits in with cyber incident reporting and regulatory harmonization generally.

Welcome back to Hacking Healthcare®.

Monthly Threat Brief

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.

Switzerland to Implement Cyber Incident Reporting for Critical Infrastructure

The Swiss Federal Council has amended their Information Security Act (ISA), and it will soon require critical infrastructure entities to report cyberattacks. Let's break down this new entry to the global list of cyber incident reporting regimes.

Incident Reporting Background

The Swiss government has been assessing and working towards introducing a cyber incident reporting mechanism for several years, and this new reporting obligation is rooted in a proposed amendment to the ISA from 2023. The increased threat of cyberattacks is the familiar catalyst for the effort, and the Swiss National Cyber Security Centre (NCSC) has stated that these reports "will enable the NCSC to assist victims of cyberattacks and alert operators of critical infrastructure."[i] The NCSC has also called the new reporting obligation a milestone for cybersecurity within the country and one that keeps it aligned with international standards.[ii]

What is Required?

Let's break down some of the key elements:

Scope: In general, the new obligations will apply to critical infrastructure sectors, but a full accounting of covered entities can be found within Article 74b of the ISA.[iii] In terms of the health sector, the reporting obligation includes:[iv]

- Health facilities listed on the cantonal hospital list pursuant to Article 39 paragraph 1 letter e of the Federal Act of 18 March 1994 on health insurance;

- Medical laboratories with an authorisation pursuant to Article 16 paragraph 1 of the Epidemics Act of 28 September 2012;

- Companies that have a licence for the manufacture, marketing and import of medicinal products under the Therapeutic Products Act of 15 December 2000;

- Organisations that provide benefits to protect against the consequences of illness, accident, incapacity for work and earning a living, old age, disability, and helplessness;

The article also clarifies that the reporting obligation “applies to cyberattacks that have an impact in Switzerland, even if the IT resources affected are located abroad.”[v]

Reporting Timeline: Covered entities will be expected to report cyberattacks to the Swiss National Cyber Security Centre (NCSC) within 24 hours “of discovery.” Additional supplemental reports may be required within 14 days to fill in missing reporting elements from the initial report.[vi]

Covered Incidents: Article 74d details what qualifies a cyber incident for reporting. An incident must be reported if it:

- Endangers the functionality of the affected critical infrastructure;
- Has led to manipulation or leakage of information;
- Remained undetected for an extended period of time, particularly if there are indications that it was carried out in preparation for further cyberattacks; or
- Involves blackmail, threats, or coercion.

Examples provided by the NCSC include “malware successfully installed on a system, encryption trojans, availability attacks,” and attacks that “[gain] unauthorised access to computer systems through the exploitation of security holes.”[vii]

Report Content & Process: Reports are to include “information on the authority or organisation required to report, the nature and execution of the cyber-attack, its effects, measures taken and, where known, the planned further action.”[viii] In order to ease the reporting burden, the NCSC will provide a reporting form on their website.

Exceptions and Protections: The stated intent of the reporting obligation is “solely” to “enable the NCSC to identify attack patterns on critical infrastructure at an early stage and thus to warn potential victims and recommend appropriate preventive and defensive measures.”[ix] As such, no one “need not provide any information in the reporting process that could incriminate him or her under criminal law,” and incidents that “have only a minor impact on the functioning of the economy or the well-being of the population” do not have to be reported.

Enforcement: While the new obligation technically enters into force on April 1, in an effort to ensure an orderly transition, there will be no enforcement of applicable fines until October 1.

Action & Analysis

Included with Health-ISAC Membership

[i] https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/meldepflicht-2025.html

[ii] https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2025/meldepflicht-2025.html

[iii] https://www.fedlex.admin.ch/eli/oc/2024/257/de#mod_u19

[iv] https://www.fedlex.admin.ch/eli/oc/2024/257/de#mod_u19

[v] https://www.fedlex.admin.ch/eli/oc/2024/257/de#mod_u19

[vi] https://www.ncsc.admin.ch/ncsc/en/home/meldepflicht/meldepflicht-info.html

[vii] https://www.ncsc.admin.ch/ncsc/en/home/meldepflicht/meldepflichtige-cyberangriffe.html

[viii] https://www.fedlex.admin.ch/eli/oc/2024/257/de#mod_u19

[ix] https://www.fedlex.admin.ch/eli/oc/2024/257/de#mod_u19

[x]https://www.reuters.com/technology/cybersecurity/hong-kong-aims-safeguard-key-facilities-with-new-cybersecurity-law-2025-03-19/

Reference(s): Reuters, , , ,
Report Source(s): Health-ISAC
Release Date: Mar 22, 2025 (UTC)

Tags: NIS2, Incident Reporting, Hacking Healthcare, European Union
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.

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