H-CSC Association Profile

Status: February 2026

1 Introduction

The “Healthcare Cyber Security Center (H-CSC)” is a national cybersecurity organization. It facilitates knowledge exchange and collaboration among healthcare institutions. Its objective is to further develop existing capabilities and create synergies to sustainably strengthen the prevention, detection, and containment of cyber incidents.

Active participation and close collaboration among members are at the core of H-CSC activities. This fosters a community of information security specialists based on mutual trust, where specialists learn from one another and work together to strengthen the resilience of the Swiss healthcare system.

2 The association

The non-profit association H-CSC was founded on 28 August 2025 by 18 Swiss hospitals with the goal of establishing a shared cybersecurity foundation for the entire healthcare sector.

Figure 1: Logos of the founding members

The H-CSC was established following a recommendation by the Swiss National Cyber Security Centre (NCSC) and directly contributes to the implementation of the National Cyberstrategy (NCS) of the NCSC. The primary strategic objective is to ensure secure digital services and infrastructures in the comprehensive sense of confidentiality, availability, and integrity.

The statutes of the H-CSC association can be downloaded from the website www.h-csc.ch.

2.1 Goals of the association

The H-CSC pursues the following objectives:

- Promoting collaboration among the cybersecurity teams of Swiss healthcare institutions
- Providing sector-specific cybersecurity solutions tailored to the needs of Swiss healthcare institutions, including those in the field of medical technology
- Reducing dependence on external providers of security solutions by building sector-specific expertise
- Establishing organizational structures for the continuous exchange of threat information and best practices
- Enabling joint procurements to strengthen negotiating power and reduce costs and effort
- Strengthening cybersecurity in medium-sized and small healthcare institutions
- Providing documents and sharing experiences with other healthcare institutions to enhance cybersecurity competencies

2.2 Bodies of the association

The H-CSC association is based on a transparent and participatory governance model that promotes strategic direction, operational efficiency, and active member participation.

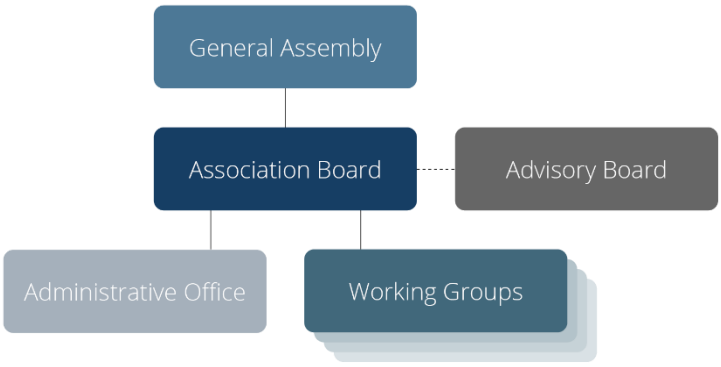

Figure 2: Bodies of the H-CSC association

The General Assembly consists of delegates from all member institutions. It elects the Board, approves results, and decides on matters such as the expansion of services.

The Association Board is responsible for the strategic leadership of the association. It is composed of seven elected members who define the association's development, supervise the Business Office, and coordinate the work of the expert groups.

The Business Office manages day-to-day operations and serves as a coordination hub for members, partners, and authorities. It supports the working groups and ensures the smooth execution of all organizational activities.

The Advisory Board ensures regular exchange between the H-CSC association and its members. This body discusses feedback on H-CSC's services and performance and gathers concrete concerns, requests, and questions from members.

The working groups consist of cybersecurity specialists from the member organizations. The Tech Team ensures the development and delivery of the association's technical services and sup-ports members in their use.

2.3 Partner

To leverage synergies and avoid duplication, the H-CSC association collaborates with several key partners from the healthcare sector and the cybersecurity industry. Current partners include the Vereinigung Gesundheitsinformatik Schweiz (VGI.ch), the National Cyber Security Centre (NCSC), and Infrastruktur Hospital Schweiz (IHS). Discussions with additional potential partners are ongoing.

2.4 Members

Membership is currently open to Swiss hospitals and clinics with a public service mandate. This includes acute care hospitals, psychiatric clinics, and rehabilitation clinics as defined by the Federal Office of Public Health (FOPH) and the respective cantons. In the long term, membership will be extended to all stakeholders in the Swiss healthcare sector in order to create a unified and resilient national ecosystem.

To become members, Swiss hospitals and clinics pay an annual membership fee to cover the costs of the services provided. The membership process is available on the website www.h-csc.ch. The H-CSC membership fee regulations and the confidentiality agreement can also be downloaded from the website.

3 Background to the establishment of H-CSC

3.1 Global threats

In an increasingly digitalized healthcare system, technology and data are essential for healthcare delivery. Cybersecurity plays a central role in ensuring patient safety, treatment effectiveness, and the protection of healthcare operations, as cybercriminals worldwide increasingly target healthcare institutions.

Healthcare organizations are attractive targets due to their reliance on interconnected systems, time-critical operations, and the potential risks to patient safety. Moreover, the use of cyber operations in armed conflicts is increasing, and critical civilian infrastructures—such as healthcare institutions—are being targeted more frequently. In recent years, both the medical sector and humanitarian organizations have been deliberately attacked, highlighting their vulnerability as part of modern digital warfare.

While cyberattacks involving ransomware or malware primarily threaten sensitive data and infrastructure in most critical infrastructure sectors, in healthcare they can also endanger human lives. In light of these threats, it is crucial that Swiss healthcare institutions strengthen their cyber resilience and are able to respond quickly and effectively to attacks. Given limited resources, collaboration among healthcare institutions is essential.

3.2 Challenges in Switzerland

Limited sector-specific expertise: General cybersecurity guidelines do not sufficiently address threats specific to healthcare institutions, such as vulnerabilities in certified medical devices, the protection of critical clinical systems containing unsupported software components, or the proper handling of sensitive

and highly regulated data under constant time pressure (e.g., in ambulances, emergency departments, or intensive care units).

High costs and effort in procurement processes: For the evaluation of IT security systems and services, nearly all healthcare institutions prepare largely identical requirements documents. In the future, such documents can be developed jointly through H-CSC and provided to members as templates. This relieves the burden on security officers, saves time and costs, and improves document quality, as lessons learned from others can be incorporated.

The H-CSC association addresses these challenges and strengthens the cybersecurity capabilities of Swiss healthcare institutions by providing sector-specific services and promoting structured collaboration across the entire sector.

4 Services

The H-CSC association provides its members with a broad range of services to support the improvement of their cybersecurity resilience, regardless of their current maturity level. These services are developed jointly with and for the members to ensure that they are tailored to the specific needs of the healthcare sector.

Currently, ten services are available to members, with most costs included in the membership fees. Most services are offered in German, French, and Italian, while some services are available only in English.

Figure 3: Overview of the H-CSC services for the members

4.1 Overview of Existing Services

- Threat intelligence collaboration & sharing: A platform for the secure and coordinated exchange of information on cyber threats, IoCs, and vulnerabilities. Members benefit from a shared situational awareness and easier integration into existing security solutions.
- Threat intelligence management: Centralized access to validated, sector-relevant information on current cyber threats. The service enables faster detection and effective prevention of attacks, reduces manual effort, and strengthens both individual and collective cyber resilience of members.
- Darknet monitoring: Continuous monitoring of relevant darknet sources for compromised credentials and sensitive information. Potential security incidents are detected and reported early, enabling affected healthcare institutions to initiate appropriate protective and countermeasures in time.

- Vendor exchange channels: Targeted exchange of experiences regarding specific vendors, products, and cybersecurity services. In dedicated channels, members share best practices and practical assessments.
- Procurement guidelines: Consolidation of members' security requirements to create a strong collective market voice. Information security is integrated early into procurement processes, contributing to more secure long-term solutions in the healthcare sector.
- Awareness campaigns: Central repository of proven awareness campaigns from members, including information on benefits, required effort, materials, and contact persons. Members can quickly identify suitable approaches and reduce their own preparation efforts.
- H-CSC conference: Annual event for networking, experience sharing, and professional development through expert presentations and discussions.
- Monthly webinars: Regular professional exchange on services, H-CSC positions, and member experience reports related to cybersecurity in healthcare.
- ERFA group for Information Security: Structured and confidential experience-sharing forum for information security leaders in healthcare institutions, targeting CISOs and IT security managers.
- Library: Central collection of proven templates, policies, and sample documents from member organizations relating to ISMS, IT baseline protection, and awareness.

This document is available in multiple language versions. In case of doubt or discrepancies, the German version shall prevail.