AMPCUS CYBER
Zero Trust Compliance Service Provider

Healthcare Technology Firm Scales HITRUST Compliance and Saves Big

www.ampcuscyber.com

OVERVIEW

A healthcare technology company, headquartered in Buchs, Switzerland, specializes in automation and supply chain solutions for hospitals and pharmacies. With over 3000 healthcare automation systems deployed worldwide in medical centers, the company aims to streamline medication management and in-facility logistics to improve operational efficiency, accuracy, and patient care.

THE SITUATION

The firm had previously achieved the HITRUST r2 certification, a key milestone demonstrating its commitment to safeguarding sensitive information. As the certification neared expiration, the company began efforts to renew and expand its compliance posture.

With the certificate expiry date fast approaching, the company faced a tight timeline to complete the assessment and meet all updated requirements. As part of this certification journey, the firm aimed to include new personnel, processes, and technologies that were excluded from the previous audit. In this latest assessment, the firm also requested that assessors evaluate the infrastructure and environment associated with its Pneumatic Tube Systems (PTS). In addition to HITRUST r2, the organization also needed to ensure compliance with HIPAA, aligning its security and privacy controls with globally recognized standards.

THE SOLUTION

Due to the tight timeline, Ampcus Cyber remained agile and collaborated with stakeholders and personnel to understand their business operations and environment, which eventually helped define the project scope. With the information gained and given that the firm was looking for multiple other standards in addition to HITRUST r2, our experts were able to tailor an approach that was unique to the organization's operational landscape.

THE APPROACH

Ampcus Cyber established a Synergised Compliance Model, which involved five phases for the successful completion of the certification journey.

Phase 1 – Train

- Conducted project kick-off meeting.
- Identified key client stakeholders and delivered a training session on controls across HITRUST and HIPAA.
- Established the Information Security Management Forum (ISMF) and Information Security Task Force (ISTF).

Phase 2 – Scope

- Defined and shared scope of assessment, including data flow, assets, and critical information.
- Created ISMS Scope Document & Statement of Applicability (SOA).
- Established project time frames and discussed dependencies and risks.

Phase 3 – Assess

- Conducted a unified gap/readiness assessment across HITRUST, and HIPAA, including control testing and evidence review.
- Developed and executed a test plan with defined sampling methods and control effectiveness criteria.
- Reviewed and uploaded policies, procedures, and evidence to the HITRUST MyCSF portal.
- Delivered a Gap Assessment Report and Action Tracker with identified vulnerabilities and mitigation recommendations.
- Initiated risk management, including asset identification, risk assessment, treatment planning, and remediation kickoff.

Phase 4 – Mitigate

- Held bi-weekly compliance team meetings to track progress, provide guidance, and drive timely gap closure.
- Used the Action Tracker Report to prioritize control implementation and remediation tasks.
- Developed and updated policies, procedures, and supporting documentation; updated the Statement of Applicability (SoA).
- Conducted internal audits, addressed non-conformities, and facilitated a Management Review Meeting (MRM).
- Evaluated and supported HITRUST r2 validated assessment readiness, including control effectiveness, scoring, evidence mapping, and sampling.

Phase 5 – Report, Audit, and Certify

- Assisted in audits for HITRUST r2, and HIPAA.
- Conducted the HITRUST r2 Validated Assessment, including internal QA, and submitted it to HITRUST for final certification.
- HITRUST r2 Interim Assessment will be done next year to ensure readiness and alignment with HITRUST requirements.
- Additionally, external audit processes (Stage 1 & 2), assisting in closing any non-conformities (NCs), and facilitating delivery of the final audit reports and certifications from external certification bodies are also part of future tasks.

NEXT STEP

- The firm is on the last leg of receiving HITRUST r2, and HIPAA certificates.
- Gap Assessment was done, and mitigations were implemented in place.
- The firm is in the process of strengthening its risk management practices and internal governance through ISMS, ISMF, and ISTF structures.

USA
Ampcus Cyber Inc., 14900 Conference Centre, Drive Suite #500, Chantilly, VA 20151.

India
601-609A, 6th Floor Beta Block, Sigma Soft Tech Park, Varthur Kodi, Whitefield Bangalore, 560066.

Philippines
Tower 3, Unit 1914, Grace Residences, Levi Mariano Avenue, Ususan Taguig City, Metro Manila 1632, Philippines.

Dubai
906-67, 9th Floor, Concord Tower, Dubai Media City, Dubai, UAE.