Acronis

WHITE PAPER

Singapore Health Information Act

C8N+FINITY

How Contfinity supports health care organisations on their HIA journey

The Singapore Health Information Act, or HIA, is reshaping how health information is contributed, protected and shared across Singapore's health care ecosystem. For many health care providers, that means preparing for NEHR contribution requirements where applicable, while also strengthening cybersecurity and data security controls across systems, access, backup and incident response.

Contfinity helps health care providers navigate HIA through a structured, practical approach that combines advisory, ongoing oversight and operational resilience. We guide organisations from understanding obligations to maintaining readiness over time.

Acronis supports this journey by providing the cyber resilience capabilities that underpin protection, backup, recovery and visibility, with Contfinity ensuring these capabilities are governed, monitored and operationalised effectively.

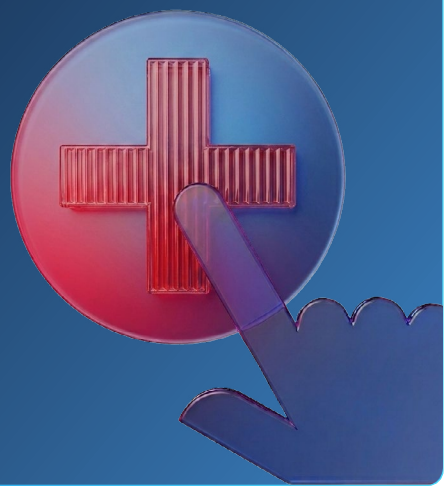
Why this matters now

HIA introduces phased obligations for licensed health care providers and retail pharmacies to contribute selected health information to the National Electronic Health Record, or NEHR, and to implement cybersecurity and data security measures to protect health information.

For providers, this extends beyond compliance alone. It is also an operational readiness challenge that affects systems, workflows, user access, backup, vendor management and incident response. Confirmed cybersecurity incidents or data breaches must be reported to MOH within defined timeframes, with an initial report due within two hours and a detailed report within 14 days.

Key things health care providers should know

- HIA was passed in January 2026, and MOH has issued implementation guidance and phased timelines for providers.
- NEHR is Singapore's national repository for selected health information across providers, designed to support safer and more coordinated care.
- HIA applies to HCSA-licensed health care providers and retail pharmacies for NEHR contribution, with cybersecurity and data security expectations extending more broadly across the health care ecosystem.
- Implementation is phased by provider type, so organisations should confirm which timeline applies to them and start preparation early.



NEHR and HIA in practical terms

NEHR contribution

Providers are required to contribute key health information according to their implementation batch and service type. This is especially relevant for health care segments where NEHR participation is still being expanded, including private specialist clinics, laboratories, dental providers and retail pharmacies.

Cybersecurity and data security

Providers are expected to implement safeguards across systems, data, access control, backup, incident response, personnel training, vendor management and organisational processes.

Important

A HIA-compliant HIMS is still required for NEHR contribution. Acronis is positioned as supporting the surrounding cybersecurity and cyber resilience measures, not as the HIMS or the NEHR integration layer.

Phased implementation timelines

Batch 1

GP services, acute hospitals, community hospitals, clinical laboratories, radiology laboratories and nuclear medicine services.

Start by: September 2027

Batch 2

Specialist outpatient medical services, nursing homes, contingency care services and outpatient renal dialysis centres.

Start by: September 2028

Batch 3

Outpatient dental services, ambulatory surgical centres, assisted reproduction services and retail pharmacies.

Start by: March 2030

How Contfinity supports the HIA journey

Contfinity supports health care organisations through a practical, structured approach to HIA readiness. We focus on helping organisations understand what applies to them, where gaps exist and how to build readiness that can be sustained over time.

- Our support spans both planning and execution, including:
- Clarifying HIA scope and applicable implementation timelines.
- Complying HIMS, NEHR readiness, operational workflows and thirdparty dependencies.
- Identifying gaps across protection, backup, access control, training, asset visibility and incident readiness.
- Developing a remediation roadmap that integrates policy, process, training and technical safeguards.
- Supporting execution and ongoing readiness as organisations move from preparation to sustained operation.

This approach helps health care providers move from awareness sustained operational action — without treating HIA as a onetime compliance exercise or purely a technology problem.

How Contfinity leverages Acronis

To help health care organisations move from assessment to sustained readiness, Contfinity leverages Acronis Cyber Protect Cloud as its core cyber resilience platform, delivered and overseen through Contfinity's CyberWatch service.

Together, these capabilities are sustained through Contfinity's ongoing oversight and support, ensuring Acronis capabilities remain effective and aligned with HIA expectations over time.

Where Acronis fits

Secure and protect systems

Acronis EDR / XDR and integrated antimalware help strengthen day to day protection across managed environments, reducing exposure to common threats faced by health care organisations.

Update and patch

Acronis RMM provides visibility, monitoring, and management capabilities that support patching and system hygiene, helping reduce risk from outdated or mismanaged assets over time.

Backup and continuity

Acronis Backup and Disaster Recovery capabilities support recoverability and continuity when systems are disrupted. Backup of essential data is a clear component of the HIA cybersecurity and data security baseline, and a critical enabler of operational resilience.

Asset visibility and oversight

Acronis improves visibility across endpoints and workloads, supporting stronger environmental awareness and more effective operational oversight.

Training and incident readiness

Contfinity combines advisory guidance with technical controls to strengthen incident readiness. Acronis supports faster detection, alerting, and response, while Contfinity defines the surrounding processes, roles and escalation paths.

Email threat protection

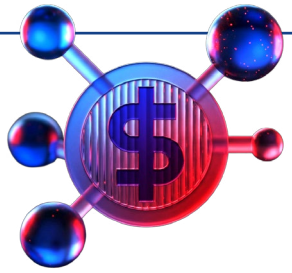
Email remains a significant source of phishing, spoofing, business email compromise and malware risk within health care environments. Acronis Email Security can be used as part of a broader effort to reduce exposure to emailborne threats in these environments.

Funding support for eligible SMEs*

Up to 70% co-funding for CISOaaS Cybersecurity Health Plan

Up to 50% Productivity Solutions Grant for Cyberwatch Plan B (Contfinity Pte Ltd).

(*subject to approval)



Disclaimer

This material is provided for general information purposes only and does not constitute legal, regulatory, or compliance advice. Health care organisations should confirm how the Health Information Act (HIA) applies to their specific circumstances and consult relevant regulatory guidance or professional advisors where required.

Acronis products and services support cybersecurity and cyber resilience measures associated with HIA readiness. They do not replace health care information management systems (HIMS), NEHR integration solutions or regulatory decision-making responsibilities.

Acronis

Learn more at
acronis.com