# Action Plan in response to the inquiry and reviews into the MMH cyber incident

| Workstream | Action summary | Detailed milestones | Milestone dates | | | |
|---|---|---|---|---|---|---|
| | | | Q1 | Q2 | Q3 | Q4 |
| **Assurance and audit** | Health NZ to work with the Ministry of Health to put in place independent assurance that the mandated standards for New Zealanders' health information security and privacy are being routinely met, through consistent sector-wide attestation, verification and review arrangements, with enforceable actions to remediate risks and issues. | 1. Health NZ to work with Ministry of Health (MOH) to investigate independent assurance arrangements. | ◇ | | | |
| | Health NZ to ensure it consistently applies cyber security and privacy, procurement, contracting, and third-party risk management policies and standards in all situations, and takes a proactive approach to assuring and documenting compliance with those requirements. | 1. Cyber security and privacy policy compliance checklist completed.<br>2. Procurement and contracting standards documentation updated.<br>3. Third-party risk management compliance audit report delivered. | ◇ | ◇ | ◇ | |
| | Health NZ to develop a plan to engage with the sector to drive better third-party security assurance outcomes across the health sector, in line with HISO and HISF Consider measures to strengthen HISF compliance among suppliers to the health sector, in particular suppliers that hold sensitive health information. | 1. Complete the review of private patent portals (x6, incl. MMH).<br>2. Sector engagement plan for third-party security assurance developed.<br>3. HISO and HISF compliance strengthening measures documented.<br>4. Updated sector compliance levels and thresholds communicated. | ◇<br>◇ | <br>◇<br>◇ | | |
| **Risk management** | Definition of thresholds and attributes for "high-risk" suppliers to the health sector; and regularly receives assurance from entities that hold contracts with "high-risk" third-party suppliers regarding their security status and HISF compliance. | 1. Health NZ will work with MOH to develop criteria for classifying suppliers as high-risk and examine options for regular assurance to monitor the security posture and HISF compliance of entities holding contracts with such suppliers. | ◇ | | | |
| | Health NZ to confirm to MOH how they manage HISF compliance and what actions have been taken in cases of non-compliance. | 1. HNZ to receive letter from MOH seeking HISF compliance confirmation requests<br>2. Health NZ prepare documentation to outline how it manages HISF compliance and actions that it undertakes where non-compliance is identified. | ◇<br>◇ | | | |
| | Health NZ to perform risk assessment across its digital portfolio as part of a systemic approach to focus remediation efforts on higher-risk data, digital systems and services, and where these are identified seek to uplift capability, close gaps, address risks and verify compliance. | 1. Establish baseline of ~10% of systems assessed at initiation.<br>2. Implement a streamlined risk assessment process (possibly automated).<br>3. Achieve ~17.5% of systems assessed by Q4. | ◇ | ◇ | | ◇ |
| | Health NZ and other health sector entities to maintain registers of their suppliers that store or process sensitive health information, tiered by risk factors (including volume of records, sensitivity, criticality to care delivery) and the associated contracts and data retention for those services. | 1. Suppliers register with sensitive health information holders created.<br>2. Risk tiering framework applied to all suppliers.<br>3. Contracts and data retention policies updated. | ◇ | ◇ | ◇ | |
| | Health NZ to comprehensively review and uplift its third-party risk management practices in-line with recommendations in the Cyber Maturity Assessment Report (Sep-25). | 1. Action plan developed based on the Cyber Maturity Assessment Report.<br>2. Complete rollout of implementation plan for Report recommendations | ◇ | | | ◇ |
| **Contracts and commercial** | Establish minimum contractual standards aligned to the new government information sharing standard. | 1. Minimum contractual standards aligned to government information sharing standard drafted.<br>2. Standards approved and published.<br>3. Standards incorporated into all new contracts.<br>4. Uplifting existing 'high risk' contracts to new compliance standards post risk assessment activity. | ◇ | ◇<br>◇ | | ◇ |
| **Delivery governance** | Formalise governance to require formal privacy and security risk assessments and assurance before piloting new projects or proceeding with procurement with documentation of risk decisions and migration strategies. | 1. Formal governance framework for privacy and security risk assessments documented.<br>2. Pre-project/procurement assurance process implemented.<br>3. Risk decision and mitigation documentation templates operational. | ◇<br>◇ | | | |

| Workstream | Action summary | Detailed milestones | Milestone dates | | | |
|---|---|---|---|---|---|---|
| | | | Q1 | Q2 | Q3 | Q4 |
| **Privacy and consent** | Strengthen PIA quality and timing to support decision-making, with a particular focus on ensuring that PIAs reflect the specific information flows and processes involved in a process, and that appropriate advice is received to ensure the quality of those PIAs. | 1. PIA quality standards and timing requirements defined.<br>2. Information flow and process-specific PIA templates developed.<br>3. PIA quality assurance review process implemented. | ◇<br>◇ | ◇ | | |
| | Enable policies such as patient or whānau notifications and consent related to storage, accessing and processing of health information to be standardised and improve patient notification in the event of a data breach. | 1. Standardised patient/whānau notification and consent policies developed.<br>2. Health information storage and access consent framework published.<br>3. Data breach patient notification process implemented. | ◇ | ◇ | ◇ | |
| | MOH and Health NZ to better define process and procedures for patient notifications in the event of data breach involving data held by a third-party supplier, with defined roles and responsibilities set. | 1. Third-party data breach notification process and procedures documented by MOH and Health NZ.<br>2. Roles and responsibilities matrix for breach notifications defined.<br>3. Joint MOH/Health NZ breach notification protocol signed off. | ◇<br>◇ | ◇ | | |
| **Cyber incident response** | Health NZ to undertake regular tabletop incident response exercises with critical suppliers that hold sensitive health data, to practice and better define incident roles and responsibilities and ensure alignment across the sector. | 1. Critical supplier list for tabletop exercises identified.<br>2. Incident response tabletop exercise schedule established.<br>3. Post-exercise improvement reports and role alignment documentation completed. | ◇<br>◇<br>◇ | | | |
| | Health NZ to continue investment in growing its cyber incident response capabilities based on improvements identified through reviews of previous or broader incident responses. | 1. Incident response capability improvement plan developed from previous reviews.<br>2. Investment roadmap for cyber incident response approved<br>3. Enhanced incident response capabilities implemented and tested. | ◇<br>◇<br>◇ | | | |
| **Manage My Health incident response** | Fully review all ongoing transfers of Northland hospitals' information to patients through the MMH portal, to provide assurance that the information is now secure. | 1. Update Health NZ interoperability strategy following MMH review.<br>2. Health NZ to deliver a vendor agnostic solution in Northland as an alternative means of sharing secondary care records to patients via patient portals. | ◇ | | ◇ | |
| | Health NZ to seek further clarification of any critical services provided to MMH by third-party suppliers, to ascertain the nature of the contract in place, and patient data accessible to third-party suppliers. | 1. Health NZ request and receive third-party supplier inventory with critical services documented from MMH.<br>2. Health NZ contract review completed for all third-party relationships to MMH.<br>3. Health NZ assess patient data access mapping for third-party suppliers to MMH. | ◇<br>◇<br>◇ | | | |
| | MMH to undertake further security reviews (penetration tests) and/or purple/red team activity on the MMH web and mobile applications. MMH to undertake a full external assessment of HISF compliance by a provider who is conversant with the HISF framework. The output of this should be provided to Health NZ as a contract holder and MOH as the health system monitor. | 1. MMH undertake penetration test and purple/red team exercise for MMH applications and report to Health NZ.<br>2. MMH engage external HISF compliance assessment report and send to Health NZ.<br>3. Assessment reports submitted to Health NZ from MMH as contract holder are shared with MOH as system monitor. | ◇<br>◇<br>◇ | | | |
| | Health NZ to seek assurances from MMH of the data management practices, aligned to HISF requirements and best practice, including details of user onboarding and offboarding processes, data retention periods, data access audit methodologies and whether patient data is accessible to any of MMH suppliers or related parties. HNZ to address remaining outstanding security and privacy items internally, and with MMH related to this incident. | 1. Health NZ requests Data management practices assurance report from MMH.<br>2. Health NZ to complete full HISF review for MMH.<br>3. Security and privacy remediation items closed out with MMH. | ◇<br>◇<br>◇ | | | |