Isle of Man Government
Reiltys Ellan Vannin

High Level Findings of Isle of Man Health & Social Care Information Governance and Data Protection Status

Summary Extract – 30 May 2022

Information and Digital Purchase Order **'IG DP Services v0.1'**: Activity 5.

Contents Page

Introduction

Following an open tender process, KPMG were selected to assist the Health Care Transformation Project team with the development and implementation of an applicable, scalable and sustainable Digital and Information Governance Framework in response to recommendations 21 - 24 of Sir Jonathan Michael's Independent Health and Social Care Review's Final Report from April 2019, in particular:

Recommendation 21: "Ensure data sharing protocols and arrangements are reviewed, agreed and implemented in accordance with the Information Commissioner's regulations and guidance."

Recommendation 22: "The development and delivery of the digital strategy should go further and faster to ensure the comprehensive capture, sharing and use of information. This would enable greater integration across the system, improved monitoring and enhanced delivery of quality and efficiency-related information."

Recommendation 23: "A core data set is essential for the management and assessment of services and should be established without delay."

Recommendation 24: "The systematic capture of accurate data should be a priority for the Island's health and care services."

In formulating our main report under Purchase Order (PO): IG DP Services v0.1 - Activity 5 we also presented other earlier reporting, namely:

1. A comparative legislative and regulatory overview and comparison between NHS England and a selection of Health and Social Care departments on the Isle of Man.

2. A document on the 'current as is' status of ROPAs within the four priority groups (Primary Care, DHSC, Public Health & Social Care – with Social Care subsequently broken down to Adult Social Care, Children & Families and Adult Social Work).

3. A report on the capacity and capability of the four priority groups to complete a ROPA and undertake delivery of the wider Information Governance Framework.

This report consolidates those findings, and further expands on them to provide a high-level overview of the current understood state of play across the health and social care system on the Island in relation to Information Governance and Data Protection.

Introduction (cont.)

KPMG was tasked under Purchase Order (PO): IG DP Services v0.1 - Activity 5 to –

Report to Project Lead findings overall in relation to ROPA, supplemented by proposal for future activity aligned with report findings to enhance the Department's Information Governance standing and solution, with proposed prioritisation if applicable. Report to include:

- Status and applicability of priority group ROPAs, inc. high-level plan for remediation.
- Summary of Data Sharing / Processing Agreements future work requirements as discovered and determined appropriate requiring remediation.
- Summary findings of Data Flows and Cross-Border transfers as determined through ROPA analysis will be presented. Will include highlighting of high-level risks, issues, gaps and concerns as found.
- Summarise LIA, PIA and DPIA future work requirements as discovered and determined appropriate requiring remediation.
- Present an overview of known in-place Information Governance relative Policies, Procedures and Guidelines future work requirements as discovered and determined appropriate, with highlighting of perceived gaps, omissions and required remedial activity requirements against a baseline Policy, Procedure and Guidelines set.
- Summarise Risk Registers (RR) future work requirements as discovered and determined appropriate requiring remediation.
- Summarise Information Asset Registers (IARs) future work requirements as discovered and determined appropriate requiring remediation.
- Asset Owner(s) (AO) mapping and correlation to IARs and required future work requirements as discovered and determined appropriate requiring remediation.
- Highlight Record Retention (RRet) procedures and activity future work requirements as discovered and determined appropriate requiring remediation.
- Highlight and summarise Information Governance Framework recommended steps to support develop of the framework based on findings of the ROPA evaluation activity and workstreams.
- High-level summary of potential applicable technical solutions to support enduring information governance will be presented.

Limitations

In formulating this high-level review, KPMG have operated within the following parameters:

- The information we have on the Isle of Man Government is based on the available information provided to KPMG by Isle of Man Government and from any publicly available sources/repositories.
- KPMG have not been in contact the Attorney General's Chambers in relation to this report.
- An information governance framework is a working document which is regularly updated. For this review KPMG has used the most up to date versions which were publicly available at the time of report writing.
- KPMG have had high level discussions with a sample of the Isle of Man Healthcare Providers; in-depth or directed discussions with the following component elements were held:
    - Primary & Community Care
    - The DHSC
    - Public Health
    - Social Care (consisting of Adult Social Care, Children & Families and Adult Social Work).

- All assessments of progress, and requirements for future progress, are made following discussions with the priority groups referenced and are based on KPMG's interpretation following discussion with the people who were present, and review of documentation provided by these individuals. KPMG sought individuals' self-assessed perceptions and discussed these during engagement sessions. It is anticipated that the individuals who were interviewed would likely agree with the assessments made by KPMG.

- There have been some delays with information being provided to KPMG, and delays in arranging workshops, which has impacted KPMG's ability to provide a complete picture of each of the priority healthcare groups as requested under this Purchase Order.

- Furthermore, since December 2021 workshops have been cancelled by the Transformation Project PM which has hindered KPMG ability to get an updated status on the priority groups ROPA and wider IG activities.

This report **does not** intend to highlight shortfalls of individuals, where they are referenced, but rather show the currently understood structure and status within the respective priority group. This is in relation to skills, capacity, awareness, and internal resourcing. KPMG are aware that there is a significant lack of capacity across all the four priority care groups in supplying and understanding the activities to support the deliverables within this Purchase Order, which has limited KPMG's ability to engage with all the priority care groups.

This report does not provide legal advice. If legal advice is required, this should be obtained by the relevant priority healthcare group from their designated legal counsel.

Summary

Against the primary areas of delivery as per the Purchase Order, we present an overview RAG status rating of those elements:

ROPA	Data Flows & Cross Border transfers	LIA/PIA	DPIA
Record Retention Procedures	Risk and Issues Registers	Information Asset Registers	Information Asset Owner(s) Mapping
Regulatory and Legislative Mapping	Data Sharing / Processing Agreements	MxC Corporate IG & DP Function	MxC – CabO: GTS SLA *
Caldicott Guardian Function *	DP & IG Operational Resource	DP & IG Policies and Procedures	Internal Data Flow Mapping
DP & IG Controls Mapped	DP & IG Skills and Competence	On Island Data Flow Mapping	Cross-border Data Flow Mapping

(* refers to linked topics not specified in Purchase Order but intrinsic to DP & IG provision)

On the following slides we have broken down the PO deliverables individually and presented some high level comments against each one respectively.

Red	• Close monitoring and or significant action/activity/resource required. The area requires ongoing frequent attention or action to enable enhancement and progress. • Area is performing with significant risk and will not be able to meet the required progress in the short to medium term without intervention and or additional resource to support resolution. • Actions in place are not believed to be enough to bring performance fully back on track in a timely manner. • Area presents a high risk and significant lack of compliance.
Amber	• Regular monitoring required. • Performance is currently not meeting the required level for the area. • Actions and activities are underway, but there remains a prevalent risk that the activity may still not be completed sufficiently or coherently. • Ongoing work may flag additional / associated issues, risks and actions to be addressed to ensure area progresses. • Area presents a medium risk and suitable lack of compliance requiring oversight and attention by management.
Green	• No immediate action required, and area is operating at a reasonably proficient level. • Periodic review advised to sustain rating.

Summary (2)

In the following table, KPMG present our high-level summary of the 'Review Areas', with general comments for consideration and an associated RAG rating.

Information Governance Area		General comments
Records of Processing Activity (ROPA)		A ROPA is a consolidated document presenting the requisite information categories to enable appropriate logging and oversight of data governance. It is also a requirement of GDPR. Based on the self-assessment undertaken by the respective priority groups, the ROPA status for each priority group is believed to be:* **Primary Care** – 1% complete (self-assessed) **Public Health** – 80% complete (self-assessed) **DHSC** – 80% complete (self-assessed) **Adult Social Care** – 5% complete (self-assessed) **Children & families** – 85% complete (self-assessed) **Adult Social Work** – 25% complete (self-assessed) * KPMG have not formally assessed, nor had sight of, these self-assessed ROPAs at the time of this summary report. KPMG therefore cannot confirm that these values are a true or realistic status, and that they are purely those values advised to KPMG and thus reported accordingly.
Data Sharing/Processing Agreements (DSA/DPA)		— KPMG have only had sight of one 'Data Sharing Agreement' which was the GTS/Manx Care Service Level Agreement. — Priority Groups were unaware of their DSAs/DPAs. Or had a log or register of their respective DSA/DPAs. — Manx Care priority groups are reliant on the Corporate DPO function, which has provided limited support on this area.
Data Flows/Cross Border transfers		None of the priority groups have undertaken a formal exercise to determine, map and record data flows.
Legitimate Interest Assessments (LIAs)		Throughout all discussions and reviews we have ascertained that no LIAs have been undertaken.
Privacy Impact Assessments (PIAs)		Throughout all discussions and reviews we have ascertained that no PIAs have been undertaken.
Data Protection Impact Assessments (DPIAs)		— It is KPMG's understanding that there is significant work required to ensure DPIAs are consistent, succinct, and adequate to meet ICO standards, and to comply with applicable legislation and regulations. A structured training program on completion of DPIAs be delivered across Business Units and Corporate Governance functions.
Policies/Procedures/Guidelines		— There is a disparate application and utilisation of policies, procedures, and protocols in relation to DP and IG. — Since its formation, Manx Care have undertaken limited activity in the creation of organisation specific policies, procedures, and guidelines. Due to the legal structure of Manx Care, Public Health and DHSC specific policies, procedures etc. need to be created that are applicable to the organisation.
Skills/Capability/Capacity		— Capacity to undertake IG & DP activities is the key limiting factor in making progress. Significant demand across the priority groups for additional personnel and resources to support the IG & DP tasks has been raised. — The skills within the various departments that KPMG have interacted with are varied, from proficient in DHSC to extremely limited in the other priority groups.

Summary (3)

Skills/Capability/Capacity (cont.)		— The overall skills, competence, capacity, and experience has been found to be far less than that expected for such an established group of organisations and those undertaking the handling, management and oversight of such extensive and sensitive data. — Overall, there is request from internal parties for relevant training to be rolled out. A full training need analysis should be undertaken by the Corporate IG & DP functions across the organisations.
Information Asset Register		Throughout all discussions and reviews we have ascertained that no Information Asset Registers have been established, nor has any evaluation to determine extent of assets been undertaken.
Asset Owner(s) Mapping		Throughout all discussions and reviews we have ascertained that Asset Owner(s) Mapping has not been undertaken.
Record Retention Policy		— KPMG have engaged with 4 departments that fall under Manx Care remit, Primary Care and 3 Social Care departments. All 4 of these departments are using an outdated DHSC Record Retention Policy. — The Manx Care Corporate IG & DP function have acknowledged that a large proportion of their policies need to be updated since the formation of Manx Care. — Public Health have provided the currently relied upon Record Retention Policy, which is the standardised Cabinet Office document, Public Health intend to adapt this document to tailor it specifically to Public Health.

Caldicott Guardian

A Caldicott Guardian's primary concern is maintaining the confidentiality of personal information collected, processed, and stored by the Isle of Man Health & Social Care on behalf of the patient. The Isle of Man Caldicott Guardian role is currently severely limited due to the lack of communication and integration of the Caldicott Guardian across the requisite areas of Information Governance and Data Protection. KPMG has noted that, at the time of assessment, the Manx Care Caldicott Guardian is currently not invited to attend the Information Governance Board.

Manx Care Corporate Information Governance and Data Protection Function

KPMG have found that the Manx Care Information Governance and Data Protection team at a 'Corporate' level have several issues ranging from inconsistent understanding of roles, to lack of capacity and capability to fulfil their positions remit. There is a foreseeable deficit in resources across the whole Isle of Man Health and Social Care Information Governance and Data Protection function, it has been raised by all functions and departments that capacity is extremely scarce, and resources are limited.

Isle of Man Health and Social Care Risk Management & Oversight

The Isle of Man Health and Social Care corporate and delivery groups currently do not appear to have, or are unable to evidence, a clearly defined risk management and oversight practice, in regards to DP & IG. Risk management should be addressed from both a tactical / patient delivery level, through to operational and up to strategic / corporate. KPMG is aware that there is a significant gap in the appreciation of the risks and issues pertaining to information governance and data protection across the health and social care domains on the Isle of Man.

Summary Findings

Summary Findings

In undertaking this high-level review, KPMG present the following findings for consideration.

A. Capacity and resource constraints are having a considerable effect on the priority groups being able to fulfil their IG & DP requirements.
B. There is a significant backlog in relation to activity required to meet regulatory obligations under the Applied GDPR. Activity that should have been undertaken prior to 25 May 2018 remains mostly not started and or is incomplete; evidence of progress made to meet the obligations prior to and post 25 May 2018 was not made available for review.
C. Lack of training in IG is profound across the Isle of Man Health and Social Care system, and in some areas, there is a significant knowledge gap in terms of understanding and ability to address IG & DP functions.
D. Clarity on job roles/responsibilities needs to be addressed and information provided from the top down.
E. Manx Care procedures, policies and guidelines need to be updated and formulated as currently there is reliance upon old DHSC documents, especially given that DHSC has acknowledged that it has identified its own necessity to update its own policies, procedures, and guidelines.
F. Caldicott Guardian role is not being effectively utilised, it is not adequately consulted or supported and does not appear to be underpinned by a defined basis (i.e. no formal basis for existing or mechanism for alignment to the equivalent function in England) in the Isle of Man.
G. The SLA between Manx Care and GTS is seen as requiring a detailed review and appropriate applicable amendments made to inaccuracies contained therein, examples are:
    i. SLA states that GTS are to enable provision of support **27**/7/365 - as this would normally be 24/7/365;
    ii. Agreement defines that there be the provision of a dedicated mail server for health and social care - this has not been provided; additionally, those GTS personnel interviewed were not aware of this provision requirement within the SLA; and,
    iii. The SLA has no defined clarification or criterion / metrics of the oversight of the SLA and the provisions contained within it.
H. GTS does not have specialist resource, nor does it have any demonstrable specialists with healthcare specific cyber security, information security and governance skills.
I. Lack of understanding of the requirements for key roles and positions across the DP & IG scheme of functions, nor evidence of appropriate informed job evaluations was not presented for review upon request.
J. Manx Care does not have a clear understanding of its regulatory, legislative and framework compliance requirements in relation to DP & IG.
K. Manx Care DP & IG function does not have a clear understanding, nor accessible record, of the controls and measures in-place across its organisation in relation to DP & IG, it does not have an audit plan, nor has it undertaken an audit of its 3rd parties, shared service providers and or vendors.
L. None of the organisations reviewed had a compiled list, nor an awareness of, the Data Sharing/Processing Agreements, in use and/or required.

Summary Recommendations

Summary Recommendations

Based upon the summary findings, and linked to wider findings throughout the review activity, KPMG's summary of the key recommendations for consideration by the Health Care Transformation Programme are as follows:

1. Seek additional personnel on a temporary surge basis to assist with the capacity issues and enable attainment of compliance.
2. A full-time increase in resources for DP & IG should be scoped and deployed across the organisations.
3. Priority Groups should continue to work on populating the ROPA sufficiently, fully, and compliantly.
4. Priority Groups should undertake to complete the full gambit of IG requirements such as mapping data flows, asset owner registers etc. in an expeditious manner.
5. Policies, procedures and guidelines across the Island's health and social care provision need to be reviewed, developed, deployed, and embedded following a full gap analysis having been undertaken.
6. Risk registers, issue logs, risk management and oversight need to be addressed through the delivery of specialist training and awareness to the required positions across the organisations.
7. A structured and disseminated communications programme should be embedded to ensure adequate communication occurs through and across all levels of the organisations.
8. Training regimen should be developed and implemented to narrow the knowledge gap and upskill applicable personnel.
9. Implementation of a formal, defined basis for the Caldicott Guardian role in the Isle of Man Health and Social Care Service and mandated alignment with the equivalent role in England, with associated policies, procedures and guidance being updated or introduced (as applicable) to underpin the role.
10. The SLA between Manx Care and GTS be revisited and a defined oversight methodology regarding KPIs, CSFs and performance metrics be implemented and reporting to the Manx Care Board should be done routinely.
11. GTS, on behalf of and in conjunction with Manx Care, should form a ring-fenced specialist team to support health and social care departments on the Island, with the resource being suitably competent and specialised in the healthcare cyber security, information security and governance domains.
12. Key roles and positions across the DP & IG scheme should undergo detailed specialist job evaluations to determine the requisite skills, experience and knowledge needed to undertake the position. *
13. Manx Care should seek support from the NHS (inc. NHS Digital) in the development of internal procedures, policies and practices with clear alignment to enable efficiencies and best practice.

*The specialist evaluations should be completed by an independent 3rd Party healthcare DP & IG specialist supplier, and not be undertaken by IoM Government internal resource from within Manx Care, DHSC, PH or OHR, for example.

Glossary

A&E	Accident & Emergency
Applied GDPR	The GDPR as applied to the Isle of Man
Applied LED	The LED as applied to the Isle of Man
BAU	Business as Usual
BS	British Standards
CAMHS	Child and Adolescent Mental Health Services
CCGs	Clinical Commissioning Groups
CDPO	Chief Data Protection Officer
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
CPO	Chief Privacy Officer
CQC	Care Quality Commission
Dept. PO	Departmental Privacy Officer
DHSC	Department of Health and Social Care
DHSS	Department of Health and Social Security
DoH	Department of Health
DoLS	Deprivation of Liberty Safeguards
DoSC	Department of Social Care
DP	Data Protection
DPA	Data Processing Agreement
DPA (UK)	The UK Data Protection Act 2018
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
DP&IG	Data Protection & Information Governance
DSA	Data Sharing Agreement
DSAR	Data Subject Access Request
FIO	Freedom of Information Officer
GDPR	The General Data Protection Regulation
GP	General Practitioner
GTS	Government Technology Services
IA	Information Assets
IAR	Information Asset Register
IAO	Information Asset Owners
ICO	Information Commissioner Office
IG	Information Governance
InfoSec	Information Security
ISO	International Standards Organisation
LED	The Law Enforcement Directive
LIA	Legitimate Interest Assessments
MxC	Manx Care
NCSC	National Cyber Security Centre
NHS	National Health Service
NHSX	NHS Digital
OCSIA	Office of Cyber Security and Information Assurance
OHR	Office of Human Resources
PH	Public Health
PIA	Privacy Impact Assessments
PMO	Project Management Officer
PO	Purchase Order
ROPA	Record of Processing Activities
RR	Risk Registers
RRet	Record Retention
SA	Supervisory Authority
ShCR	Shared Care Records
SLA	Service Level Agreement
SIRM	Senior Information Risk Manager
SIRO	Senior Information Risk Owner/Officer
SISO	Senior Information Security Officer
SME	Subject Matter Expert
WHO	World Health Organisation