mentalwelfare commission for scotland

dignity & rights ethical care respect ca & equality

CORPORATE REPORT

Information governance, technology and systems development strategy 2017/20

JUNE 2017

Information governance, technology and systems development 3 year strategy - 2017-2020

Context

This document details the Information Governance and Technology Strategy for the Mental Welfare Commission for Scotland over the next three years.

In addition to the IG&T strategy the Commission has the following related policies which are reviewed and updated regularly

- Data Protection Policy
- Information Risk Management Policy
- IT Security Policy
- IT Code of Conduct
- Mobile Devices Policy
- Records Management Policy

Our drivers

This document describes the role IG&T and our primary system, or Information Management Portal (IMP), plays in the delivery and realisation of the Commission's goals and how this underpins the Commission's overall strategy.

The Commission's aim is to protect and promote the human rights of people with mental health illness, learning disabilities, dementia and related conditions. Our duties are set out in mental health law.

Performance Management

For each of the Commission's key activities there are a set of defined key performance indicators (KPIs). The Commission's information governance framework and IT systems both play a significant part in providing the data required to measure performance against these KPIs and publishing performance indicators.

Information Governance & Technology

"Information Governance & Technology" comprises our technical equipment and systems. It also includes the provision of a secure environment which ensures that the Commission can undertake data processing safely. The data which is processed and

managed allows the Commission to fulfil its statutory monitoring duties and also provides management to assist informed decision making.

"Information Governance" assures the confidentiality, integrity, availability and protection of information (service user, staff, financial, organisational) in paper or electronic format.

The Commission strives to ensure that its own information technology and governance arrangements reflect current good practice as set out in current, relevant NHS Scotland and Scottish Government Guidelines **(see Appendix A).** The Commission's IG&T strategy has to take cognisance of wider initiatives within both government and the NHS, including, for example, an increasing emphasis on interoperability, data sharing as well as current digital transformation initiatives.

These overarching strategic documents have to be read and understood within the context of the Commission as a small organisation and that, while our approach to IT and IG security is diligent, that some measures described in these papers must be scoped appropriately for smaller organisation with limited staffing complement and finite resources.

The National Confidential Forum

Scottish Ministers passed legislation which established the National Confidential Forum (NCF) in spring 2014 as a Committee of the Commission. The Commission was, as a consequence, heavily involved in the set up arrangements for the NCF. The Commission continues to support the NCF's IT capability as well as supporting it in maintaining sound records management and data protection practice.

Sustainability

The Commission publishes its annual sustainability report in October each year. As part of the Government's targets for sustainability, there is a focus on reducing the carbon footprint of IT systems. The Commission is also committed to exploring different methods for enabling electronic methods for sharing forms and notifications and move away from paper forms.

As we await a move across to using an encrypted email server as standard (NHS Mail 2), we can start to look at other processes that may benefit from using this secure way to transfer data. Potentially this could enable the Commission to work more sustainably by ceasing transmission of some paper forms and notifications and could potentially reduce costs associated with postage or couriers.

Strategic Timetable

This is a high level plan of activity for the next 3 years. It encompasses 3 areas of activity;

- Information Governance
- Information Technology
- Information Systems (IMP)

Current Year – Apr 2017 to Mar 2018

Year 1: Information Governance
Create an action plan detailing the activity required to ensure our house is order in advance of full implementation date of the new EU General Data Protection Regulation in May 2018 (GDPR)
Formalise and document arrangements for the storage and retention of personal, sensitive data gathered as part of our investigations and more detailed casework.
Alongside HR colleagues, use the new LMS, LearnPro, to deploy and develop training programmes to ensure implementation of new data handling and records management core competencies and a training register.
Knowledge Management: practitioners will be developing new content as Part 2 of the Q & A project. This content will reflect, amongst other things, the new MHA. Upload the new Q & As and provide training for practitioners to ensure that they are able to update/revise Q&A content on the Intranet. This will enhance and refine knowledge capture and encourage reuse.
Initiate the development of an Information Asset Register with appropriate guidance for asset owners and a structured meeting arrangement
Continue to support and provide guidance for NCF colleagues
Further establish a security incident register and ensure that this is maintained and reports are submitted to the Audit Committee of the Commission.
Report progress concerning our Records Management Plan to the Keeper (National Records of Scotland) making use of the new template.
Establish the role of Data Protection Officer (DPO) & ensure that the role and relative responsibilities are clear.

Year 1: Information Technology
Effect the final migration to NHS mail 2.
Embed project methodology for larger IT initiatives supported by the OIMs role at the Commission
If time permits, undertake a needs analysis for Board members around how MWC communicates and shares papers and documents and devise a plan to make this more streamlined, secure and effective
Maintain all servers, including those at NCF, keeping them secure and up to date; maintain remote access for all users; maintain network security; monitor the back-ups, ensuring that the data is valid and the external drives are stored securely; and maintain laptops, ensuring that they are secure and patched.
Provide advice and support for imminent changes to the office accommodation and facilitate any changes which are agreed.
Investigate potential for making cost savings from within the IT budget by exploring opportunities within Scottish Government framework agreements

Year 1: Information Systems
Complete development of v7 MHA forms and provide input to any promotion of the new forms/Act.
Develop IMP SQL queries and code for monitoring/reporting and for maintenance, to accommodate v7 forms and the new Act
Develop advance statement register
MHTS missing forms - develop technical process for 'close loop' checking of MWC receipt of missing forms, eradicating any need for casework admin visual inspection.
Observe and monitor IMP's performance as new Act goes live, making in-house technical modifications as necessary and liaising with Servelec on any issues with their code.
Liaise with colleagues to tailor IMP to support new team structures and ways of working
Investigate Tableau software to develop automatic, interactive and live presentation of IMP management and monitoring data using dashboards.
Actively engage with other organisations, e.g. ISD on data linkage projects.

Refine our open Data Plan and, working with Communications colleagues, identify which of our monitoring data sets could be made available online in a more open format (Excel, CSV)

Year 2 – Apr 2018 to Mar 2019

Year 2: Information Governance
Finalise the Information Assets Register. Assign owners and a support framework of meetings and supporting documentation
By March 2018, implement action plan created for the new EU General Data Protection Regulation.
Develop, monitor and evaluate the implementation of training in data handling and records management
Work with colleagues at NCF to establish a clear plan as to what will happen to NCF information assets following the closure of the Forum, working closely with staff from NRS and other bodies to ensure this is in line with current guidelines and best practice.

Year 2: Information Technology
Explore functionality provided by NHS mail and look to exploit this within the Commission (e.g. potential of a new mobile phone platform, Skype for business, use of instant messaging option)
IMP servers will be reaching their end of life so need to plan and deliver the IMP hardware replacement project. Need to scope out how to replace the 5 IMP servers and how we would fund this. ***(This exercise may fall into year and be brought forward to the early part of 2018 depending on the budget situation at this point in time.)***
This would require an installation of the latest Windows server operating system (which might be Windows server 2016 or a later version depending on testing outcomes between 2016 – 2018)
The IIMP system runs on SQL server. Need to review the need to install the latest version of SQL server. This project would require assistance from CSE Servelec.
Create an evidence based business case around migration to the Scottish Wide Area Network (SWAN)
Start replacing desktops and laptops this would mean all machines would be running Windows 10 ***(This action is necessary but may be subject to change depending on any decision regarding MWC accommodation.)***
Explore opportunities (outside SWAN network) for usage of secure, government approved cloud storage opportunities.
Maintain all servers, keeping them secure and up to date; maintain remote access for all users; maintain network security; monitor the back-ups, ensuring that the data

is valid and the external drives are stored securely; and maintain laptops, ensuring that they are secure and patched.
Work with NCF to ensure the proper decommissioning of IT equipment at the Glasgow office, recycling equipment where possible or ensuring that that it is disposed of in line with current best practice.

Year 2: Information Systems
Observe and monitor IMP's performance as new Act goes live, making in-house technical modifications as necessary and liaising with Servelec on any issues with their code.
Review IMP 'notification requiring review' and workflow alerts to check fitness for purpose/ adherence to the Act, modifying where necessary. This, in conjunction with the following item will reduce MWC time spent investigating false positive alerts.
Develop software tools & processes to monitor the quality of Verifying, offering feedback to casework admin to improve our confidence in data pulled straight from IMP and reduce faulty data cleanup time.
Presentation of live IMP data - investigate and develop facilities (e.g. in Excel) to offer automatic, interactive and live presentation of IMP management and monitoring data, e.g. using dashboards.
Engage with other organisations, e.g. ISD on data linkage projects.
Investigate technical/ process methods of reducing, by automation, staff workload.
Liaise with OPG on the significant differences between their guardianship prevalence figures and ours.
Explore opportunities for more streamlined data transmission with other bodies (e.g. the newly formed Scottish Courts service)
Work with IT and Servelec on IMP Hardware Refresh Project (the upgrade of server hardware/ operating system/ SQL server version).

Year 3 – Apr 2019 to Mar 2020

Year 3: Information Governance
Explore opportunities for utilising open source software or small proprietorial system to more effectively manage our corporate and non-service user records
Develop asset owner's role and ensure that there is adequate training and recognition of the role at MWC
Prepare for formal re-evaluation of our Record Management Plan (RMP) by the Keeper of the National Records of Scotland as 2019 will mark 5 years since the Commission's RMP was approved on a continuous improvement basis
Work with colleagues at NCF to deploy the plan for the closure of the Forum's office, redeploying equipment where possible and ensuring that records are either retained or securely destroyed as appropriate

Year 3: Information Technology
Benchmark the Commission against other, smaller public authorities in relation to digital maturity.
Consider replacement of corporate firewall, depending on any decision taken regarding joining the SWAN network.
Maintain all servers, keeping them secure and up to date; maintain remote access for all users; maintain network security; monitor the back-ups, ensuring that the data is valid and the external drives are stored securely; and maintain laptops, ensuring that they are secure and patched.

Year 3: Information Systems
Work with Police Scotland to automate transmission of POS1 data from their new database, developing a software interface to translate police data into a format suitable for automatic insertion into IMP, thus negating the need for MWC to 'key' pos data.
Engage with other organisations, e.g. ISD on data linkage projects.
Explore opportunities for more streamlined data transmission with other bodies (e.g. the newly formed Scottish Courts & Tribunal Service)

Appendix A

Notes:

It is important that the Commission keeps up to date with published guidance and best practice in the field of information governance and technology and strives to be the best it can be. Much of the literature published is aimed at organisations that are considerably bigger than the Commission and so we have to be mindful to aim for the achievable and that we scope recommendations in the literature to match the resources available to us.

1. NHSS Information Security Policy Framework

The NHSS Information Security Policy Framework replaces both the NHSS Information Security Policy (2006) and the NHSS Information Assurance Strategy (2011-2015).
The new framework differs from the former policy in terms of purpose, scope and construction in the following ways:

- For the first time there is a commitment to conforming to the International Standard ISO-27001 (2013) across all Boards as closely as possible (though it is not a requirement to be formally certified).
- From February 2015 the Information Commissioner Office (UK) has statutory powers to audit and inspect any NHSS Health Board with or without notice. It has been agreed that where such as audit is to occur, the NHSS Information Security Policy Framework and associated controls will be used as a starting point to establish non-conformance to NHSS policy and adherence to the provisions of the Data Protection Act (1998) (especially but not exclusively seventh principle).
- It is not possible to have a single standalone information security policy as in the past. Instead, each Board is responsible for its own information security policy and information security objectives but must include a number of national mandatory 'components' that are agreed by eHealth Governance structures (e.g. eHealth Strategy Board)
- These components include the need to formally plan, build and implement an information security management system (ISMS), to make leadership and resource commitments between 2015 and 2017
- Some of the mandatory components are the national controls, standards and guidance which featured prominently in the previous Information Security Policy (2006). The national control set/standards/guidance need to be constantly updated (e.g. email, encryption, online tools).

2. DL (2015) 17 - Information Governance and Security Improvement Measures 2015-2017

Director's letter distributed by John Matheson CBE, Director of Finance, eHealth & Analytics, introducing the new framework and stressing the importance of sound security.

Alison Aiton

Information Governance and IT Manager

May - 2017

Thistle House
91 Haymarket Terrace
Edinburgh
EH12 5HE
Tel: 0131 313 8777
Fax: 0131 313 8778
Service user and carer
freephone: 0800 389 6809
enquiries@mwcscot.org.uk
www.mwcscot.org.uk

Mental Welfare Commission (Jun 17)