

Public Records (Scotland) Act 2011

State Hospitals Board for Scotland (Carstairs)

The Keeper of the Records of Scotland

31st July 2017

Contents

1. Public Records (Scotland) Act 20113
2. Executive Summary4
3. Authority Background4
4. Keeper’s Assessment Process.....5
5. Model Plan Elements: Checklist.....6
6. Keeper’s Summary25
7. Keeper’s Determination25
8. Keeper's Endorsement..... 26

1. Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) received Royal assent on 20 April 2011. It is the first new public records legislation in Scotland since 1937 and came fully into force on 1 January 2013. Its primary aim is to promote efficient and accountable record keeping by named Scottish public authorities.

The Act has its origins in *The Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950-1995* (The Shaw Report) published in 2007. The Shaw Report recorded how its investigations were hampered by poor record keeping and found that thousands of records had been created, but were then lost due to an inadequate legislative framework and poor records management. Crucially, it demonstrated how former residents of children's homes were denied access to information about their formative years. The Shaw Report demonstrated that management of records in all formats (paper and electronic) is not just a bureaucratic process, but central to good governance and should not be ignored. A follow-up review of public records legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

The Act requires a named authority to prepare and implement a records management plan (RMP) which must set out proper arrangements for the management of its records. A plan must clearly describe the way the authority cares for the records that it creates, in any format, whilst carrying out its business activities. The RMP must be agreed with the Keeper and regularly reviewed.

2. Executive Summary

This report sets out the findings of the Keeper's assessment of the RMP of the State Hospitals Board for Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 22nd December 2016.

The assessment considered whether the RMP of the State Hospitals Board for Scotland was developed with proper regard to the 14 elements of the Keeper's statutory Model Records Management Plan (the Model Plan) under section 8(3) of the Act, and whether in this respect it complies with it and the specific requirements of the Act.

The outcome of the assessment and the Keeper's decision on whether the RMP of the State Hospitals Board for Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

In 1994 legislation went through Parliament to bring The State Hospital legally into the National Health Service in Scotland as a Special Health Board - The State Hospitals Board for Scotland - accountable to Scottish Ministers through the Scottish Government. The State Hospital is one of four high secure hospitals in the UK. Located in South Lanarkshire in central Scotland, it is a national service for Scotland and Northern Ireland. 75.5% of the patients are 'restricted' patients within the jurisdiction of Scottish Ministers. That is a patient who because of the nature of his offence and antecedents, and the risk that as a result of his mental disorder he would commit an offence if set at large, is made subject to special restrictions without limit of time in order to protect the public from serious harm.

<http://www.tsh.scot.nhs.uk/>

4. Keeper's Assessment Process

The RMP was assessed by the Public Records (Scotland) Act Assessment Team on behalf of the Keeper. Assessors used the checklist elements listed in section 5, to establish whether the State Hospitals Board for Scotland's RMP was developed with proper regard to the elements of the Model Plan and is compliant with the Act. The assessment also considered whether there was sufficient supporting evidence of such compliance.

Key:

G	The Keeper agrees this element of an authority's plan.		A	The Keeper agrees this element of an authority's plan as an 'improvement model'. This means that he is convinced of the authority's commitment to closing a gap in provision. He will request that he is updated as work on this element progresses.		R	There is a serious gap in provision for this element with no clear explanation of how this will be addressed. The Keeper may choose to return the RMP on this basis.
----------	--	--	----------	--	--	----------	--

5. Model Plan Elements: Checklist

State Hospitals Board for Scotland (Carstairs) (for simplicity this authority will be referred to as 'the Board' in the assessment below)

Element	Present	Evidence	Notes
1. Senior Officer <i>Compulsory element</i>	G	G	<p>The State Hospitals have identified James Crichton, Chief Executive, as the individual with overall responsibility for records management in the authority.</p> <p>Mr Crichton is the Board's Accountable Officer.</p> <p>This appointment is confirmed in the State Hospitals' <i>Health Records Management Policy</i> (section 5.3) (see element 3).</p> <p>The Chief Executive's overall responsibility for records management in a health board is an idea supported by principles in the <i>Scottish Government Records Management NHS Code of Practice (Scotland)</i>: http://www.gov.scot/Resource/Doc/366562/0124804.pdf</p> <p>Mr Crichton approved, and has signed, the <i>Records Management Plan</i> (the <i>Plan</i>).</p> <p>Mr Crichton is responsible for the hospital's compliance with the Data protection Act 1998 (see Data Protection Policy – see element 9 – page 9). He is also responsible for the security of all systems (see I.T. Policy – see element 8 - section 1.6.1)</p> <p>The Keeper agrees that the State Hospitals Board for Scotland has identified an appropriate individual to this role as required by the Public Records (Scotland) Act</p>

			2011 (the Act).
2. Records Manager <i>Compulsory element</i>	G	G	<p>The State Hospitals Board have identified two individuals to this element. While recognising that the Act would indicate the identification of a <u>single</u> individual, the Keeper has agreed that shared responsibility is acceptable practice in this particular sector due to the clinical/administrative structure of some health boards.</p> <p>The State Hospitals Board has identified Robin McNaught, Finance & Performance Management Director and Dr Duncan Alcock, Associate Medical Director/Caldicott Guardian as the individuals with day-to-day responsibility for implementing the <i>Records Management Plan</i>.</p> <p>Mr McNaught is the Board’s SIRO.</p> <p>This identification of the Caldicott Guardian to this role is confirmed in the State Hospitals’ <i>Health Records Management Policy</i> (section 5.4) (see element 3). The Caldicott Guardian, alongside other relevant officers in the hospital “work together to ensure there are agreed systems for Records Management...” (<i>Plan</i> page 5). No Health Record can be altered without the approval of the Caldicott Guardian (<i>Health Records Policy</i> section 18). The Caldicott Guardian is responsible for advising staff and ensuring adequate security arrangements regarding the hospital’s compliance with the Data Protection Act 1998 and for maintaining confidentiality generally (I.T. Policy – see element 8 – section 1.6.2)</p> <p>As Finance and Performance Manager, Mr McNaught is the ‘owner’ of the <i>Plan</i> and is a member of the State Hospitals Board. He is also the ‘lead Director for Risk Management’ (Business Continuity Planning Framework – see element 10 – page 5).</p> <p>The Caldicott Guardian is responsible for the review of the <i>Health Records Policy</i></p>

			<p>(see element 3) which should take place in 2017.</p> <p>The Board have provided the Keeper with a letter from the Board’s Chief Executive confirming the above arrangements.</p> <p>The Keeper agrees that the State Hospitals Board has identified appropriate individuals to this role as required by the Act.</p>
<p>3. Policy <i>Compulsory element</i></p>	<p>A</p>	<p>G</p>	<p>The Board have a <i>Health Records Policy</i> which has been supplied to the Keeper. This is version 2.0 approved by the Senior Management Team and implemented from June 2014.</p> <p>The Board have an <i>Management, Retention & Disposal of Administrative Records Policy</i> which has been supplied to the Keeper. This is version 1.0. dated February 2007. However, the Board have stated “The current Administrative Records Policy is outdated and requires some work to bring it up to an acceptable standard. This work has begun and will be completed in 2017.” This work features in the Action Plan against this element (and against element 5). The Keeper agrees this action and requests that he is sent the updated Policy when it becomes available. The Board have committed to do this.</p> <p>Both <i>Policies</i> are simultaneously operational and are complementary.</p> <p>The <i>Health Records Policy</i> is the responsibility of the Associate Medical Director (see element 2).</p> <p>The Board have provided the Keeper with screen-shots to show that these policies are available to staff on their intranet.</p> <p>The Keeper is able to agree this element of the Board’s <i>Plan</i> under</p>

			<p>improvement model terms. This means that the authority has identified a gap in their records management provision (the administrative records policy is out-of-date) and have put processes in place to close that gap. The Keeper's agreement is conditional on his being updated as the new <i>Administrative Records Policy</i> becomes available.</p>
<p>4. Business Classification</p>	<p>A</p>	<p>G</p>	<p>The <i>Health Records Policy</i> (see element 3) notes that “The ability to identify and locate information is essential to the delivery of high quality evidenced based care.” (section 1).</p> <p>The <i>Scottish Government NHS Code of Practice</i> published at http://www.gov.scot/Publications/2012/01/10143104/0 states that “An effective records management service ensures that information is properly managed and is available whenever and wherever there is a justified need for information...”</p> <p>The Board operates a hybrid paper/electronic system.</p> <p>Paper is kept in an in-house ‘Main Health Records Department Store’ with clear tracking in place (see element 11). Locally, active records are held in ‘hubs’.</p> <p>A programme of scanning is taking place uploading patient records to the Electronic Patient System (Rio). This process is explained in appendix 4 of the <i>Health Records Policy</i> (see element 3).</p> <p>The Board hold electronic records in line of business systems and in local shared drives.</p> <p>The Board states (<i>Plan</i> page 10): The intention is to create a hospital-wide system which will incorporate all departments and systems. It is recognised that this is a huge undertaking and will take time and resources to put in place, however</p>

			<p>commitment is there to see this project through” - N.B. the Chief Executive has signed the <i>Plan</i> and therefore can be directly associated with this commitment. The Board have provided a small sample of how this system might look (from the finance department). The Keeper agrees that, with an organisation the size of the State Hospital, it is inevitable that progress will be made on an incremental basis. The Board have separately informed the Keeper that Work is underway although at a very early stage. The Keeper will expect to see continual progress over the next year or so.</p> <p>The Board intend to engage with local service areas in the roll-out of the new system. The Keeper commends this principle as likely to produce a stronger business toll for the authority.</p> <p>The Board have provided their departmental filing arrangements (for administrative records) as Appendix 1 of the <i>Management, Retention & Disposal of Administrative Records Policy</i> but have noted that this document is out-of-date (see element 3). These ‘filing arrangements’ provide a strong, information asset register style, business tool featuring retention, details of storage, destruction and access conditions against record types. This should prove useful when creating the ‘hospital wide system’ referred to above (obviously only for administrative records).</p> <p>The <i>Plan</i> notes (page 6) that a third party, Patients Advocacy Service, operate in the hospital under a service level agreement. A copy of this agreement has been provided to the Keeper.</p> <p>The Board have an <i>E-Mail Policy</i> which has been supplied to the Keeper as part of the <i>Information Security Framework</i> (see element 8).</p> <p>The Keeper is able to agree this element of the State Hospital Board for Scotland’s Records Management Plan under ‘improvement model’ terms. This</p>
--	--	--	---

			means that the authority has identified a gap in their records management provision (No formal, hospital-wide, business classification scheme), but have put processes in place to close that gap. The Keeper's agreement is conditional on his being updated on the progress of the improvement plan explained above.
5. Retention schedule	G	G	<p>Retention decisions around record series held by the Board feature in the <i>Health Records Policy and Management, Retention & Disposal of Administrative Records Policy (for both see element 3)</i>.</p> <p>The retention schedules for clinical and administrative records are based on the guidance available in the <i>Scottish Government NHS Code of Practice</i>. The adoption of the Code is noted in the <i>Health Records Policy (see element 3)</i> section 18. The Keeper notes that a new version of this Code should be available soon and assumes that the Board will adopt any material changes the new Code introduces.</p> <p>The Board have provided the Keeper with a screen-shot showing that staff can access retention schedules on their intranet.</p> <p>The Keeper agrees that the State Hospital Board have an approved and operational retention schedule that covers the expected record types created by a health board.</p>
6. Destruction Arrangements <i>Compulsory element</i>	A	G	<p>The <i>Scottish Government NHS Code of Practice</i> states that NHS Boards should be able to "...define the process of managing records throughout their lifecycle, from their creation, usage, maintenance and storage to their ultimate destruction or permanent preservation"</p> <p>With this in mind the Board has the following procedures in place for the destruction</p>

			<p>of records:</p> <p><u>Paper (internal)</u>: Paper records are destroyed under contract with a third party shredding company. An e-mail and letter, proving that these arrangements are operational, has been supplied as evidence.</p> <p>Section 18.2 and Appendices 11 and 13 of the <i>Health Records Policy</i> (see element 3) explains the destruction of scanned paper copies of health records (see element 4 for scanning project). The destruction of the original health record is done under the supervision of the Caldicott Guardian (see element 2).</p> <p><u>Paper (external)</u>: There is no indication that The Board holds records with a third party storage supplier.</p> <p>The Keeper agrees that the authority has procedures in place to irretrievably and securely destroy paper records.</p> <p><u>Electronic Records</u>: The <i>Plan</i> states “There are no formal arrangements in place currently for the destruction of electronic data...” but goes on to commit the Board to “Look at how electronic data should be destroyed in line with the <i>Business Classification Scheme</i>.” This latter statement is lifted from the Action Plan against this element. The Keeper agrees this action. The development of a hospital-wide solution for electronic records (see element 4) will greatly assist this aspect of destruction. Monitoring the imposition of retention decisions (see element 5) will be fundamental in mapping the success of this project.</p> <p>The Keeper notes that ‘housekeeping’ of e-mails features in the <i>E-Mail Policy</i> (section 3.4.8) and this includes instructions to delete. The E-Mail Policy is part of the <i>Information Security Framework</i> (see element 8).</p>
--	--	--	---

			<p><u>Hardware</u>: Hardware is destroyed, via the e-health department, under contract with a third party shredding company. An e-mail, proving that these arrangements are operational, has been supplied as evidence. Details also appear in the <i>Data Protection Policy</i> (see element 9) page 9 and the <i>I.T. Policy</i> (see element 8) section 1.6.7.</p> <p><u>Back-Ups</u>: The Board, quite properly, take back-up copies of records for business continuity reasons. However, there is no indication in the <i>Plan</i>, or in the evidence documents for business continuity, how long back-up copies are kept. The Keeper requires clarification regarding this as it is imperative that the Board is clear as to how long copies of records remain available after the ‘originals’ are destroyed. The Board have provided an explanatory e-mail from the Board’s head of e-health explaining the authority’s back-up cycle.</p> <p>The Keeper is able to agree this element of the State Hospitals Board’s Records Management Plan on improvement model terms. This means that an authority has identified a gap in their records management provision (in this case that electronic records are not universally destroyed at the end of their retention period), but have put processes in place to close that gap. The Keeper’s agreement is conditional on his being updated as the project explained in element 4 is progressed.</p>
<p>7. Archiving and Transfer <i>Compulsory element</i></p>	<p>A</p>	<p>G</p>	<p>The <i>Health Records Policy</i> (see element 3) supports the idea of records being selected for permanent preservation (see section 1).</p> <p>The State Hospitals Board for Scotland have identified the National Records of Scotland (NRS) as the appropriate repository for records identified as suitable for permanent preservation.</p>

			<p>A Memorandum of Understanding regarding the transfer of records from the Board to NRS is being negotiated at the time of this assessment. This is confirmed by the NRS Client Management Team.</p> <p>The Keeper agrees this element of The State Hospitals Board for Scotland’s <i>Records Management Plan</i> under ‘improvement model’ terms. This means that he acknowledges that the authority has identified a gap in provision [there is no formal transfer agreement with the archive] and have put processes in place to close that gap. The Keeper’s agreement is conditional on his PRSA Assessment Team being provided with a copy of the signed MOU when available.</p>
<p>8. Information Security <i>Compulsory element</i></p>	<p>G</p>	<p>G</p>	<p>The Caldicott Guardian (see element 2), alongside other relevant officers in the hospital “work together to ensure there are agreed systems for Records Management including managing the confidentiality and security of information and records within the State Hospital” (<i>Plan</i> page 5).</p> <p>To this end, the Board has an <i>Information & Network Security Policy</i> (the <i>IS Policy</i>) which has been supplied to the Keeper. This is version 5.0 approved by the Senior Management Team in January 2016.</p> <p>This is a framework made up of suite of policies such as the <i>Internet Policy</i> and the <i>I.T. Equipment Policy</i>.</p> <p>The Board have set themselves the target of being fully compliant with ISO 17799, ISO 27002 and the NHS Security Policy and Standards.</p> <p>The Board have provided an <i>Addendum to Clinical and Admin Records Policies</i> which provides staff instructions regarding the protection of information on vacating offices, decommissioning buildings and terminating staff contracts.</p>

			<p>The <i>Health Records Policy</i> (see element 3) explains the physical security in place for records in-situ or while being transported. The Keeper agrees these appear thorough.</p> <p>The physical security of servers features at section 1.6.7 of the <i>I.T. Policy</i>.</p> <p>The Board have provided the Keeper with a screen-shot showing that staff can access these policies on their intranet.</p> <p>The Keeper agrees that the Board have procedures in place that appropriately ensure information security in the authority.</p>
9. Data Protection	G	G	<p>The State Hospitals Board for Scotland have a <i>Data Protection Policy</i> which has been supplied to the Keeper. This is version 4.0 approved by the Senior Management Team April 2016.</p> <p>The Policy states: “The Board” regards the lawful and correct treatment of personal data as very important to the successful delivery of the highest quality of service. The lawful and correct processing of personal information is a key part to building trust and confidence between The State Hospital and those it deals with.”</p> <p>The <i>Data Protection Policy</i> explains the (current) 8 principles of data protection.</p> <p>The <i>Data Protection Policy</i> provides flowcharts as staff guidance on the processing of patient identifiable information .</p> <p>The authority is registered with the Information Commissioner: Z567052X</p> <p>The plan states that the State Hospitals are currently working on subject access</p>

			<p>request guidance. The <i>Data Protection Policy</i> states that “all individuals are aware of their rights...” (section 9). Detailed guidance appears as section 14 of the Health records Policy (see element 3). The Board have provided a Screenshot of website and patient leaflet attached as evidence.</p> <p>The Plan specifically states that the Data Protection Act 1998 is a “key statutory requirement” (page 5).</p> <p>The Keeper agrees the <i>Data Protection Policy</i> is supported by the <i>Information & Network Security Policy (see element 8)</i>.</p> <p>The Board have provided the Keeper with a screen-shot showing that staff can access these policies on their intranet.</p> <p>The Keeper agrees that the State Hospitals Board have appropriately considered their responsibilities under the Data Protection Act 1998.</p>
<p>10. Business Continuity and Vital Records</p>	<p>G</p>	<p>G</p>	<p>The State Hospitals Board has an overarching <i>Business Continuity Planning Framework</i> (provided version 3 - July 2007) and separate business unit (Department) <i>Business Continuity Plans</i> which describe local provision. A sample of one of these local <i>Plans</i> has been provided. The Keeper agrees that these consider the recovery of information and vital systems.</p> <p>This supports the IT Security Policy commitment (section 1.3) that “Business Continuity Plans are produced, maintained and rested.” See also I.T. Policy section 1.6.7 and 1.7.3. None of these sections details the retention period of back-up copies (see element 6).</p> <p>A requirement to test the Business Continuity Arrangements is stated in the I.T. Policy (see element 8) section 1.8.</p>

			<p>The Board have provided the Keeper with a screen-shot showing that staff can access these policies on their intranet.</p> <p>The Keeper agrees that the State Hospitals Board for Scotland has procedures in place for the recovery of records in the event of a 'disaster'.</p>
11. Audit trail	A	G	<p>Within the Health Records Department an electronic tracking system is used to book records in and out of the department. Within the hub areas, tracer cards are available to record any movement.</p> <p>With regard to electronic records, the Patient Administration System (RiO) records all updates to records, ensuring that the most current version is always available with archive history in the background. The Keeper agrees that line of business systems operated by the authority have tracking functionality (for example RIO). He also notes the submission in evidence of the hospital's clinical case note tracking system.</p> <p>The <i>Health Records Policy</i> goes into the tracking of clinical records in sections 9, 10 and 11. There may be no equivalent for non-health records. This may be acceptable as an improvement model as the work explained at element 4 is pursued. To this end the Board state: Further work to be carried out with regard to tracking of non-clinical records and version control. This will be undertake and part of the Business Classification Scheme work by a select group of staff. Work is expected to being in June 2017.</p> <p>The Board have supplied, in evidence, Tracer cards and electronic tracking systems guidance; system audit function information and a <i>Corporate Document Standards</i> document.</p>

			<p>The Keeper agrees this element of the Board’s <i>Plan</i> under ‘improvement model’ terms. This means that the authority has identified a gap in provision (in this case that controlled record tracking is limited by the absence of a Business Classification/File Plan), but the Keeper is convinced that they have instigated processes to close that gap (see element 4). The Keeper’s agreement is conditional on his being updated as the project explained in element 4 is progressed.</p>
<p>12. Competency Framework for records management staff</p>	<p>G</p>	<p>G</p>	<p>The State Hospitals Board have provided the job profile of the Finance and Performance Director and details of the relevant training undertaken by this officer and by the Caldicott Guardian (see element 2).</p> <p>The Keeper agrees that these individuals have the appropriate responsibilities, experience, seniority and objectives to implement the Records Management Plan.</p> <p>The Scottish Government Records Management NHS Code of Practice (Version 2.1) states (section 34): "All staff, whether clinical or administrative, should be appropriately trained so that they are fully aware of their personal responsibilities as individuals with respect to record keeping and management"</p> <p>Training features as section 17 in the Board’s <i>Health Records Policy</i> (see element 3) which makes the following commitment: “Staff will receive record management training as deemed appropriate by their departmental manager...” and goes on to note that update sessions will be offered.</p> <p>All staff have to undertake patient confidentiality training and sign a confidentiality clause on induction.</p> <p>The Board has a 4 part information governance training suite details of which have been provided to the Keeper. One module is specifically on records management.</p>

			<p>These appear to be mandatory (<i>Health Records Policy</i> section 17). The Keeper commends this.</p> <p>The Board's <i>I.T. Security Policy</i> commits the authority to ensure their staff are "adequately trained in their security related roles and responsibilities" (section 1.6.10) and "I.T. Security training is given to all staff." (section 1.3). Also sections 1.6.5 etc. The Keeper commends the emphasis on staff training in Information Security.</p> <p>The Board are investigating the possibility of information governance training both external (IHRIM) and in-house.</p> <p>The Keeper agrees that the individuals identified at element 2 have the appropriate responsibilities to implement the <i>Plan</i> and that there is clear accessibility to relevant training for this officer. Furthermore he agrees that information governance training is made available to appropriate staff.</p>
<p>13. Assessment and Review</p>	<p>G</p>	<p>G</p>	<p>The Act requires a scheduled public authority to "keep its records management plan under review" (part 1 5.1 (a)).</p> <p>The State Hospital Board have committed to review their <i>Plan</i> at least on an annual basis and reports on its implementation are to be passed to the Board (also annually).</p> <p>The Board intend to involve their Clinical Effectiveness (internal audit) team in reviewing particular elements of the <i>Plan</i> and this team's worksheet has been provided showing that retention and destruction will be reviewed in the winter of 2017. The Keeper notes that this proposal is 'draft' at the moment. However, he accepts that this probably relates to timing rather than intention. That said, he requires the Board to inform him if this self-assessment mechanism does not</p>

			<p>proceed.</p> <p>The Board have also committed to collate the results of the Plan review using the Keeper’s own PUR (progress update review) mechanism. This will allow reports to be returned to the Keeper and to the Board’s senior management in a structured format.</p> <p>The Keeper acknowledges that policies and procedures submitted in evidence have review dates included in their control sheets and commends this:</p> <p>The <i>Data Protection Policy and Procedures</i> (see element 9) is due for review by April 2017.</p> <p>The <i>Hospital Access & Egress Procedure</i> (see element 8) is due for review by May 2017.</p> <p>The <i>Health Records Policy and Procedures</i> (see element 3) is due for review by June 2017.</p> <p>The <i>Incident Reporting and Review Policy</i> is due for review before September 2018.</p> <p>The <i>Information & Network Security Policy Pack</i> (see element 8) is due for review by January 2019.</p> <p>The <i>Safe Use of Medicines Policy and Procedures</i> is due for review by November 2019.</p> <p>The <i>Information sharing between The State Hospital & the Police</i> document was due for review by June 2016 and <i>The Technology and Electronic Devices Within The State Hospital</i> policy should have been reviewed by February 2016. The Board</p>
--	--	--	---

			<p>state: "This is the most current, up to date policy. It has been noted that it requires updated and this will be taken forward by eHealth staff."</p> <p>The State Hospital's registration with the Information Commissioner (see element 9) must be renewed before 23 August 2017.</p> <p>A requirement to test the Business Continuity Arrangements is stated in the I.T. Policy (see element 8) section 1.8.</p> <p>The Keeper agrees that SEStran have processes in place to keep the <i>Plan</i> under review as required by the Act. Furthermore, he agrees that other information governance documents have review periods imposed as required.</p>
<p>14. Shared Information</p>	<p>G</p>	<p>G</p>	<p>"The duty to share information can be as important as the duty to protect patient confidentiality" (Caldicott principle 7 https://nhsns.org/pages/corporate/caldicott_guardians.php)</p> <p>This principle is reflected in the <i>NHSScotland 2020 Workforce Vision</i>: that NHS Boards should "work seamlessly with colleagues and partner organisations". The Board quotes this part of the vision in its Annual Report 2015/16: http://www.tsh.scot.nhs.uk/Board/Docs/TSH%20Annual%20Report%20-%20main/TSH%20Annual%20Report%202015-16.pdf</p> <p>In order to help fulfil these aspirations the State Hospital has agreements in place with other authorities such as South Lanarkshire Council and the Mental Health Tribunal (<i>Plan</i> page 5).</p> <p>The <i>Plan</i> states (page 23) "Where there is a regular requirement to share between organisations, an Information Sharing Protocol and Service Level Agreement is negotiated."</p>

			<p>A sample <i>Information Sharing Policy</i> has been provided to show that staff instructions are available in the case of “irregular but expected” information sharing requests.</p> <p>A extract from a <i>Service Level Agreement</i> has been provided showing an example of the information governance clauses applied.</p> <p>In the Action Plan against this element the Board have committed to ensure that information sharing agreements are put in place for any relevant sharing projects in future. The Keeper agrees this action.</p> <p>The Keeper has noted that NHS Scotland will shortly be delivering a mandatory <i>Information Sharing Toolkit</i> and the Keeper would expect the Board to adopt this when it becomes available.</p> <p>The <i>Plan</i> states that NHS Scotland undertakes information sharing in line with the Data Protection Act 1998.</p> <p>The Keeper agrees that The State Hospitals Board properly consider information governance when entering into arrangements to share information with third parties.</p>
--	--	--	--

State Hospital Board for Scotland (Carstairs)
(for simplicity this authority will be referred to as 'the Board' in the assessment below)

General Notes on RMP, Including Concerns:

Version:

This assessment is on the *Records Management Plan* (the *Plan*) of The State Hospitals Board for Scotland version 1.1 dated 09/06/2017.

The *Plan* is signed by James Crichton, Chief Executive (**see element 1**) and dated December 2016.

In the introduction, the *Plan* provides an explanation of records management in the authority and of the Public Records (Scotland) Act 2011.

The *Plan* mentions the Public Records (Scotland) Act 2011 (the Act) and is based on the Keeper's, 14 element, Model Plan <http://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan>.

Third Parties:

The Act makes it clear that records created by a contractor in carrying out a scheduled authority's functions are public records (Part 1 section 3.1 (b)).

The Board clearly state (Plan page 26): "No third party organisation carries out functions on behalf of The State Hospitals Board for Scotland."

Information Governance Group (IGG):

The IGG is chaired by the State Hospital's Senior Information Risk Owner. Its membership includes representation from a broad range of service areas. The *Records Management Plan* is a standing agenda item for meetings of this group. The group includes the Caldicott Guardian (**see element 2**), the Health Records Manager, the Data Protection Officer and others. The IGG reports to the Board.

A sub-group of the IGG will be responsible for the major reworking of the hospitals records management system explained under element 4 above.

Another sub-group of the IGG is responsible for reviewing and updating the *Management Retention and Disposal of Records Policy* (**see element 3**).

Members of the IGG will provide IG advice to staff when required and for developing and imposing information security and data protection arrangements in the hospital (*I.T. Policy* section 1.6.8 and *Data Protection Policy* page 8). They review the *Data Protection Policy* annually.

The IGG produces an annual report which is presented to the Clinical Governance Committee.

The IGG advised on the Information Security Framework (**see element 8**).

It is clear that this group have a fundamental part to play in the records management procedure in the authority and the Keeper thanks the Board for detailing their role.

6. Keeper's Summary

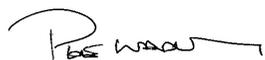
Elements 1 - 14 that the Keeper considers should be in a public authority records management plan have been properly considered by the State Hospitals Board for Scotland. Policies and governance structures are in place to implement the actions required by the plan.

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper **agrees** the RMP of the **State Hospitals Board for Scotland**.

- The Keeper recommends that the State Hospitals Board for Scotland should publish its agreed RMP as an example of good practice within the authority and the sector.

This report follows the Keeper's assessment carried out by,



.....
Pete Wadley
Public Records Officer



.....
Robert Fotheringham
Public Records Officer

8. Endorsement of Report by the Keeper of the Records of Scotland

The report has been examined and is endorsed under the signature of the Keeper of the Records of Scotland as proof of compliance under section 1 of the Public Records (Scotland) Act 2011, and confirms formal agreement by the Keeper of the RMP as submitted by the State Hospitals Board for Scotland. In agreeing this RMP, the Keeper expects the State Hospitals Board for Scotland to fully implement the agreed RMP and meet its obligations under the Act.



.....
Tim Ellis
Keeper of the Records of Scotland