NHS
Borders

Information Governance Committee
Annual Report

2015/16

Contents

Introduction

This is the ninth NHS Borders Information Governance Annual Report, and covers the financial year 2015/16 to meet the Board's Governance Reporting cycle.

Information Governance is the framework within which we manage the information we hold as an organisation. The main principles aim to ensure that we handle information in a confidential and secure manner to appropriate ethical and quality standards. Information Governance covers all types of information and is the responsibility of all staff.

The work is underpinned by the following:

- The Data Protection Act 1998
- The Freedom of Information (Scotland) Act 2002
- The Public Records (Scotland) Act 2011
- Confidentiality: NHS Scotland Code of Practice
- Records Management
- Information Security Standard
- NHS Data Quality Assurance (Data Accreditation)
- Caldicott Guardianship

With the introduction of several public WiFi hotspots and social media for business use, revisions have been made to the Internet policy to reflect these. Enhancements were made to the Subject Access Process to reaffirm the health professionals' key role in authorising the release of personal information.

A new LearnPro module has been developed based on the Information Governance Code of Conduct. This is scheduled to be published over the next Quarter and is to further remind NHS Borders staff of information governance matters.

These are just some of the key achievements made over the year and we aim to improve the level of compliance with the Information Governance Standards by keeping our staff well informed about their responsibilities, and providing an effective governance structure within which to work.

Much of the year ahead will be taken up with implementing elements of the NHS Borders Records Management Plan that was developed during 2015/16 as specified under the Public Records (Scotland) Act 2011. In addition, there will be a significant amount of resource required to progress compliance with the NHS Scotland Information Assurance Strategy Framework.

June Smyth
Executive Director for Information Governance

1 Overview

Information Governance is a strategic framework to ensure guidance and best practice is applied to the way we handle information, as an organisation and as individual members of staff. Information governance encompasses the following work strands:

- Confidentiality
- Caldicott
- Data Quality Assurance
- Data Protection
- Freedom of Information
- Information Security
- Records Management
- Staff training and awareness

Information Governance covers all types of information and is the responsibility of all of NHS Borders staff, both clinical and non-clinical.

1.1 Information Governance Standards

The NHS Scotland Information Governance Standards were first published in November 2005 and monitored nationally until 2012 using a toolkit to assess the various elements.

In 2010/11, it was agreed that NHS Borders had achieved Level 2 for all ten standards in the Toolkit, with policies, procedures and training schedules in place. Since 2012, active monitoring against the toolkit has been discontinued. Progress has continued to be made through the Information Governance Work Plan.

No further work has taken place nationally to release a new toolkit. However, as part of the 2015 – 2017 Information Assurance Strategy, there is a new Information Assurance Framework. It is being proposed that this framework is used in place of a toolkit by all NHS Scotland organisations to demonstrate compliance and best practice.

1.2 Information Assurance Strategy

In November 2011, the Scottish Government first published a four year NHS Scotland Information Assurance (IA) Strategy which set out the strategic direction for further developing the IA capability and effectively embedding an IA culture across NHS Scotland.

The Strategy identified key outcomes and actions to be taken at a national and a local level to support the developments from the eHealth strategy. Most of the actions set out in the strategy at a national level were developed in consultation with health boards to support the eHealth Strategy. The actions have been mapped against what was in place within NHS Borders, to prioritise areas for attention.

With the 2015 – 2017 Information Assurance Strategy now released by the Scottish Government, the Information Governance direction of travel for the coming year and beyond has now been established for NHS Borders.

2 Structure

2.1 Information Governance Team

The Information Governance team was established in March 2009 and reports to the Information Governance Committee. It is managed by the Senior Health Information Manager and comprises the Information Governance Lead and the Information Governance Officer.

2.2 Information Governance Committee

The Committee met on four occasions in the year. The main business of the meetings has been carried out following a standing agenda incorporating the following elements:

- Information Governance Action Plan - exception reporting
- Information Governance Incident Reporting
- Freedom of Information
- Information Security
- Records Management and Data Quality
- Staff Awareness and Training
- Internal and external papers for consultation

Details of the Information Governance Committee membership are provided in Appendix 1, and meeting attendance in Appendix 2.

3 Policy & Planning

3.1 Records Management Strategy & Policy

Both the NHS Borders Records Management Strategy and Policy were reviewed in 2015 as part of Public Records (Scotland) Act work. The revised versions were approved by the Information Governance Committee in December 2015.

The Information Governance Policy has been revised to include reference to the Environmental Information Regulations. Compliance with the policy in terms of learning and signing confidentiality statements is now part of Clinical Board Performance Review Scorecard targets.

Key performance indicators were agreed by the IG Committee and continued to be reported on during 2015/16.

3.2 Information Governance Action Plan

Having moved away from the Information Governance toolkit, the IG Team have amalgamated the action plans for information assurance, records management, information security and information governance onto one work plan. Through this, the IG Team manage the work and provide exception reports to the Information Governance Committee.

Most of the year has been taken up with developing and producing the Records Management Plan as required by the Public Records (Scotland) Act 2011. The draft Plan was submitted to the Keeper of the Records of Scotland on time, at the end of January 2016. Acceptance of the Plan is expected from the Keeper during Q1/2 2016/17.

The IG team has also worked on a range of other issues during the year. These include:

- **Redeveloping the LearnPro training module** – This is based on the content of the Information Governance Code of Conduct, complementing the detail within that. It is scheduled to be published during Quarter 2 2016/17.
- **Updated the Information Governance Committee ToR –** Based on comments received by senior managers and discussions with other Boards the Terms of Reference for the Committee have been comprehensively revised with the Committee now reporting to the Clinical Executive Ops Group.

- Mobile Device Policy – Work continued on the development of a policy to define the use and security of "ultra" mobile devices, such as smartphones, tablets and similar products. This policy incorporates a "BYOD" element to cover personally owned devices. Local guidance is in place and has been issued to IT Services to follow when considering the introduction of any such devices to the organisation.
- Secure e-mail Guide – The Secure E-mail Guidance was updated following a move by the Scottish Government to change their e-mail domain to gov.scot. This was necessary to address the issue that mails to the new domain from NHS Mail addresses do not travel over a secure route and so were not approved for sensitive or confidential information
- Voice recognition devices – It was identified that the voice recognition devices used for dictation of patient notes were not configured in a way that was consistent with the NHS Scotland secure mobile data policy. Following discussions an agreement was reached to implement a unique PIN for each device and extend the timeout time period to 1 hour. These settings are now being applied to the entire estate.

3.3 Information Governance Code of Conduct for Staff

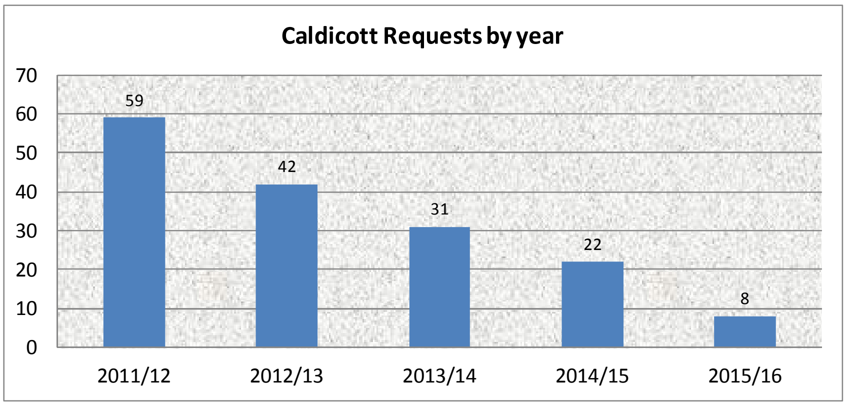
The NHS Borders Information Governance Code of Conduct for Staff, accompanied by new confidentiality statements and supported by an e-learning package, was formally launched in April 2011.

The Code was comprehensively revised during 2014/15 with a significant amount of work done to clarify the guidance on the removal of patient notes from Health Board premises. This covered instances where notes are needed in satellite clinics or patient homes, etc. The approval process for transporting notes was also simplified.

During 2015/16 the Information Governance team met with several different groups of staff, including GP staff, to deliver awareness training.

4 Caldicott Guardianship

Over the last year there were 8 applications for access to patient identifiable information which is a further significant drop on the previous year. This is largely due to requests being handled centrally by the Public Benefit and Privacy Panel which was set up by the Scottish Government and NHS Scotland. The Information Governance team lead is obliged to participate in these panels on two or three occasions per year with each attendance requiring a significant amount of work prior to the panel date.



Of these 8 requests, 3 were from IM&T staff wishing to access data. Other requests were concerned with audit (2), access by a relative (1) and other types of requests (2).

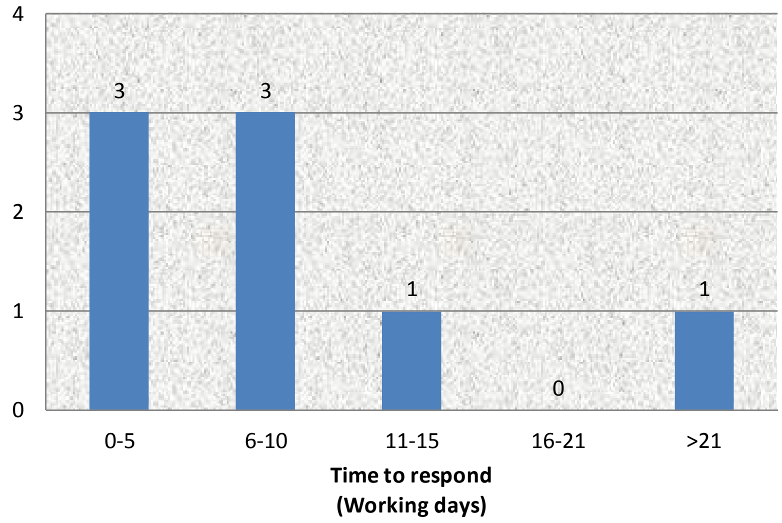
The table below shows that all 8 applications were approved, but only after conditions were applied or further safeguards to protect data security and confidentiality were agreed.

Table 4.1: Outcome of applications to the Caldicott Guardian, 2015/16

	Conditions specified		No Conditions specified		Total	
	Number	%	Number	%	Number	%
Approved	8	100%	0	0%	8	100%
Refused	0	0%	0	0%	0	0%
Total	8	100%	0	0%	**8**	100%

Generally applications that have conditions specified take longer to process as they need further investigation and scrutiny. Potentially this could contribute to the application going beyond the 15 working day target to process. The chart below shows performance against this target with all but one of the applications processed within 15 days, hitting the target.

Chart 4.1: Time to process Caldicott applications, 2015/16



5 Records Management

Public Records (Scotland) Act 2011

The work to address the requirements of the Public Records (Scotland) Act (PR(S)A) has dominated the Information Governance team's time over the past year.

Progress on the RMP to date includes:

- The formation of a Project Group that represents all areas of the organisation
- The creation of a Local Records Manager guidance document
- Completion of a Gap Analysis at a departmental level to establish the measures currently in place and to identify the areas each department will need to address to achieve corporate compliance
- Raising awareness of the fundamental changes to records management that the implementation of the RMP will impose

The current NHS Borders Records Management Policy sets out the principles of records management as well as schedules for maintaining, archiving and destruction of all types of records used by NHS Borders. This will be reviewed to ensure it meets the requirements of the Public Records (Scotland) Act 2011.

6 Subject Access Requests

Under the Data Protection Act, staff and patients (and their legal representatives) have the right to review the information which is held about them by an organisation. These requests are managed and monitored as “Subject Access Requests.”

The numbers of requests received by the Subject Access team continues to increase with a stepped increase around the time of the introduction of the Patient Rights Act Scotland 2011; as can be seen in chart 6.1.

Chart 6.1: Subject Access Requests by Category 2006/07 – 2015/16

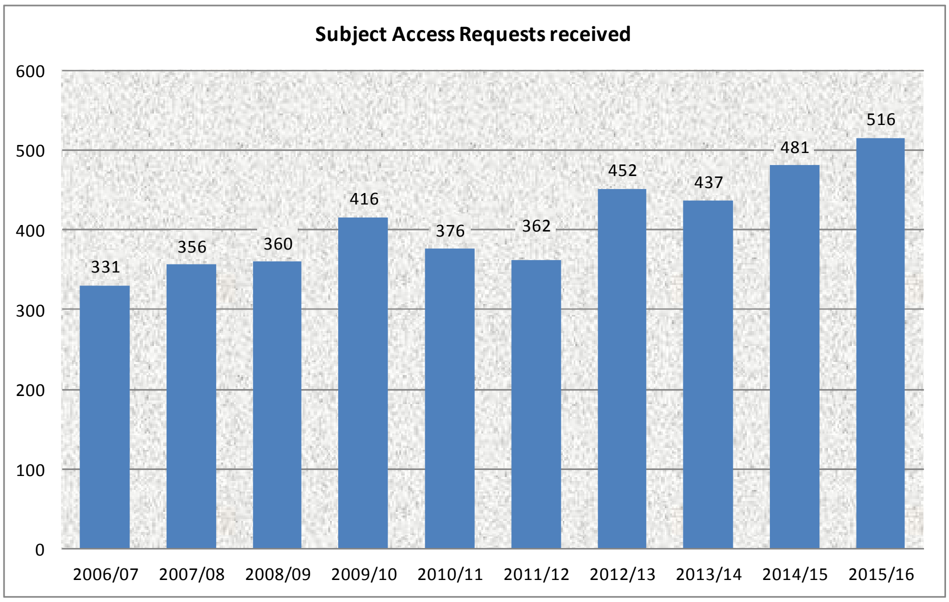


Chart 6.2: Subject Access Requests by Quarter 2015/16

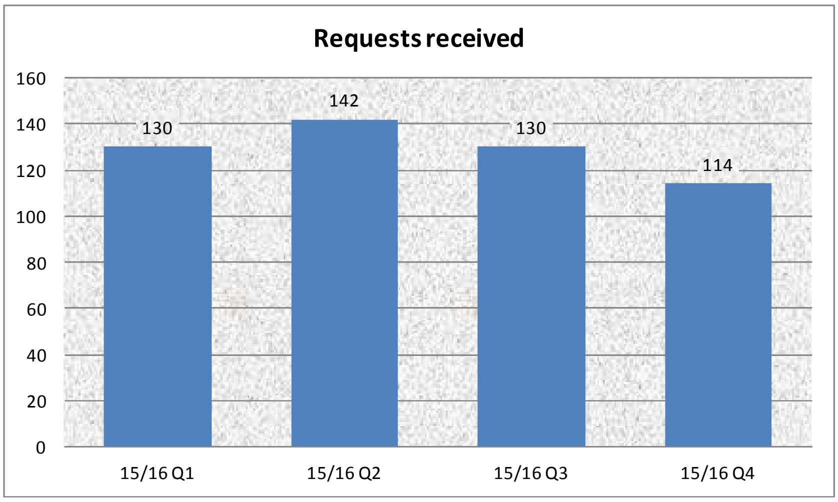
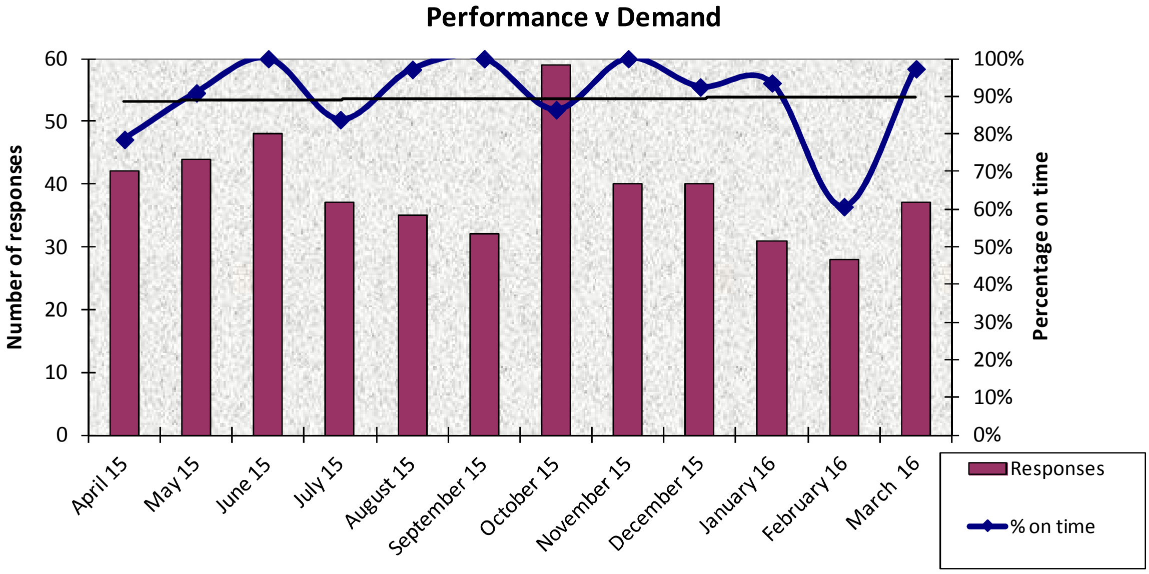


Chart 6.2: Subject Access Requests by Quarter 2015/16

Capacity within the Subject Access Request coordination team can impact on the ability to respond to all requests within the timescales stipulated by the Act. The chart below combines the number of requests responded to with the timescale compliance rate per month. Overall for the year, compliance was 90%.



7 Data Sharing

The Information Governance team was involved in reviewing the Pan Lothian/Borders Data Sharing Protocol. No changes were made to this document however Health and Social Care Integration will result in more data sharing agreements and procedures being developed over the next 12 months. It is likely that the Scottish Government preferred SASPI (Scottish Accord on the Sharing of Personal Information) model will be adopted in due course.

8 Information Security

As information technology has become essential in the management of information, it is necessary to ensure there are safeguards in place to enable information to be shared electronically with the right people without compromising confidentiality. This includes the accuracy and completeness of information, the safety of computer systems and software and preventing and minimizing the impact of system malfunctions.

Work has continued to formalise policies and protocols used within IM&T to ensure the systems run effectively across the organisation, and to ensure all staff are aware of their individual responsibilities for information security.

8.1 Standards and Guidance Documentation

Information Governance has a comprehensive library of standards, policies and guidance documents. Where appropriate, these are available on the Information Governance intranet page. During 2015/16 work continued to revise and update theses documents in accordance with good practice guidelines.

8.2 Mobile Computing

Progress has been made to pilot the use of handheld devices such as smartphones and tablets to support clinical care. It is important that information security be maintained with these, and the Information Governance team has developed technical security policies, in line with national guidelines, to ensure this is the case. This is a fast developing area and it is expected that ongoing work will be required in 2016/17.

8.3 Privacy Breach Detection Project

FairWarning remains the privacy breach detection tool used within NHS Borders and has now been in operation, providing daily reports, for 4 years.

The clinical information recording systems and patient management systems used within NHS Borders log the activity of users accessing the systems. FairWarning works by importing this information on a daily basis and collates reports according to predetermined categories, such as staff looking up their own records, or those of neighbours or family. These potential breaches of policy are checked to see whether the staff member is involved in the patient’s care or administration. If not, they are forwarded to the appropriate line manager for further investigation.

The number of potential incidents (those where the predefined criteria were met) identified by FairWarning was down by 7% during 2015/16 on the previous year’s figures. Of the 9,141 potential incidents only 132 cases were referred to line management for further investigation. This is up 11% on the previous year. As shown in the tables below, the number of confirmed incidents was also up: 12% higher than the previous year.

The increase in confirmed incidents has resulted in an awareness campaign being undertaken, with several communications issued via different methods through the year (Team Brief, Staff Update, Information Governance microsite, Featured Advert, etc.).

The breakdown of the confirmed incidents is shown in the tables below.

Table 8.1: Privacy breach detection investigations and outcomes

2012/13

Access Type	Amount
Self	82
Address	17
Family Member	23
Co-Worker	1
Total	**123**

2013/14

Access Type	Amount
Self	44
Address	4
Family Member	11
Co-Worker	1
Total	**60**

2014/15

Access Type	Amount
Self	29
Address	4
Family Member	5
High Profile	4
Co-Worker	2
Total	**44**

2015/16

Access Type	Amount
Self	40
Address	0
Family Member	3
High Profile	2
Co-Worker	5
Total	**50**

9 Incident Reporting

Breaches of data protection and information security are reported through Datix, the NHS Borders electronic incident reporting system. The system provides a record of the incident and the follow up actions and allows members of the Information Governance Team to track and follow up the actions taken. Each incident is investigated, and where appropriate, relevant action taken to address the specific issue. Generally this has involved providing additional education and awareness.

In November 2013 a major update to Datix was implemented and the opportunity was taken at this time to rationalise the Information Governance incident categories. This piece of work made it easier for incident reporters to select the correct category thus simplifying the summary reporting considerably. Appendix 3 shows the new categories and examples of incidents that fit each category.

The table below summarises the incidents reported over the past 12 months. The previous 2 years have also been included for comparison. While most incident categories have shown reduced numbers there was a 9% rise in the total number of reported incidents over the past 12 months. This is most due to a 38% increase in the number of staff viewing their own health records and an 18% increase in the reported cases of misfiling.

Table 9.1: Summary of Types of Incident

Incident class	Incident Summary	2013/14	2014/15	2015/16
Breach of Confidentiality	Confidential information emailed to inappropriate destination	5	1	6
	Confidential information found in public/inappropriate place	15	8	8
	Confidential information sent to wrong recipient	22	33	17
	Confidential waste left insecure	4	1	2
	Information divulged carelessly	7	2	6
	Information divulged intentionally	1	2	1
	Permitted password to be used by other person	1	2	1
Breach of Confidentiality Total		55	49	**41**
Failing to Secure	Confidential information emailed without appropriate security	0	1	1
	Confidential information sent but not received	2	1	2
	Hardcopy confidential information sent using inappropriate method	3	1	2
	Hardcopy confidential/sensitive data lost/misplaced/stolen	20	16	11
Failing to Secure Total		25	19	**16**
Inappropriate Access	Accessed acquaintance/friend record (FairWarning)	1	0	0
	Accessed clinical records without due reason (Not FW)	1	2	3
	Accessed family member record (FW)	6	2	2
	Accessed other person's record inappropriately (FW)	1	1	3
	Accessed own record (FW)	23	20	32
	Accessed work colleague record (FW)	0	3	4
	Used password of other person	1	1	0
Inappropriate Access Total		33	29	**44**
Incorrectly filed	Patient documents/labels found in wrong record	61	44	47
	Patient documents/labels not filed at all or not in correct place in record	5	2	9
Incorrectly filed Total		66	46	**56**
Grand Total		179	143	**157**

Table 9.2: Summary of Incident by Reporting Clinical Board

Clinical Board	2013/14	2014/15	**2015/16**
Acute	114	83	93
Learning Disabilities	1	2	1
Mental Health	13	4	19
Primary Care	19	13	16
Support Services	32	41	28
Grand Total	179	143	**157**

10 Freedom of Information

The Freedom of Information (Scotland) Act 2002 (FOISA) was introduced in January 2005. The Act requires all public authorities in Scotland to make any information they hold available on request. The FOI(S)A protocol is reviewed annually to ensure issues are addressed and to take account of developments in the FOI(S) system.

Each year since its introduction, there has been has been a steady increase in the number of requests. The majority of requests continue to relate to the performance of the NHS and particularly to the impact of Government cuts in funding and how this has impacted on Health Boards at a local level.

10.1 Activity

The volume of FOI requests slightly dipped with 2015/16 seeing a decrease of 0.5% on the previous year. Requests from the media continue to account for the highest volume of work at 37% with those from the Scottish Parliament accounting for 23%. The other categories have all roughly stayed the same.

10.2 Response Times

The Act requires that all requests are responded to within 20 working days. During the year 2015/16 our compliance slightly decreased to 98%.

The main reason for this decrease in compliance rate was the complexity of the FOI requests and the time it takes to secure final approval.

We continue to actively monitor and take action to ensure breaches are kept to a minimum and support departments to respond to requests within the required timescale. Wherever possible, the applicant is informed in advance of the likely delay and this helps to reduce the likelihood of the applicant complaining to the Scottish Information Commissioner.

Table 10.1: Compliance with statutory deadline

	2015/16	*2014/15*	*2013/14*	*2012/13*	*2011/12*	*2010/11*
Total number of requests responded to	503	527	331	399	326	331
Number of requests answered within 20 working days	497	524	243	325	292	298
Number of requests answered in more than 20 working days	6	3	88	74	34	33
Median number of days taken to respond	14	12	20	19	18	18
Percentage compliance	**98%**	**99%**	**74%**	**81%**	**90%**	**90%**

A full list of all the requests made to NHS Borders can be found on the Information Governance intranet site and on the NHS Borders website.

10.3 Reviews & appeals

Applicants who are unhappy with the response they receive or the way in which the response was handled may ask for a review of their request. If they remain dissatisfied, they may appeal to the Office of the Scottish Information Commissioner.

In 2015/16, eight applicants requested NHS Borders undertake an internal review of the handling of their request. Of these cases five responses were upheld and the other three were partially upheld.

There was one appeal to the Office of the Scottish Information Commissioner received in this time period. The Commissioner found NHS Borders had failed to comply with section 15(1) of FOISA (Duty to provide advice and assistance). Further details are available on the following link:

http://www.itspublicknowledge.info/ApplicationsandDecisions/Decisions/2015/201501218.aspx

10.4 Performance monitoring

Quarterly activity reports are produced for the Information Governance Committee. These reports detail the requests made, our response times for answering the requests and where exemptions are applied, among other performance indicators. These reports are published on the staff intranet and the NHS Borders website.

In order to comply with the spirit of the Act, it is important to ensure the use of exemptions is kept to a minimum. The default position is disclosure and when exemptions are considered, the risks and benefits are taken into account as part of the process. The most common reasons for not providing the applicant with the requested information are that it is already available elsewhere, usually on NHS Borders' or another organisation's website. The other main reason an exemption will be applied by NHS Borders is due to the fact we are a small Board and where the data relates to individual people, whether patients or staff we are bound by the Data Protection Act 1998 not to provide data on any statistic that is less than 5, therefore we are required to withhold under Section 38 of the FOISA. This is also in accordance with the Code of Practice for Official Statistics any number that is less than five, actual numbers and potentially identifiable information is withheld to help maintain patient confidentiality due to potential risk of disclosure. Further information is available in the ISD Statistical Disclosure Control Protocol.

Table 10.2: Outcome of requests

	2015/16	***2014/15***	***2013/14***	***2012/13***	***2011/12***	***2010/11***
All information released	***222***	***202***	200	190	165	188
Information part released	***206***	***152***	84	137	115	107
Information not held	***109***	***83***	67	122	19	77
Information withheld – cost of compliance	***27***	***31***	41	83	40	31
Exemptions applied	***139***	***90***	22	46	27	26
Vexatious request	***0***	***0***	0	0	0	0
Other (further clarification requested and not provided, invalid request, request withdrawn, redirected)	***9***	***7***	9	10	11	2

Note: some responses fall into more than one category

11 Training & Awareness

Training and awareness remains key to successful information governance within any organisation, as much of the national guidance and legislation for information governance is of a technical and detailed nature. Whilst improved IT solutions continue to be put in place, the success of these is in part dependant on staff compliance, and for compliance, staff need to be fully aware of their information governance responsibilities.

In 2015/16, in addition to a number of articles on information governance published in the Corporate Team Brief, Staff Update and IM&T Bulletin, emails have been issued widely across NHS Borders to highlight specific hot topics and the desktop "post-it" and Intranet Featured Advert have been utilised several times.

11.1 eLearning

All NHS Borders staff members are required to be fully familiar with the concepts and principles of information governance. As well as providing face to face training and awareness sessions, an e-learning package is available as part of the suite of mandatory training provided to staff. It includes basic learning in data security, confidentiality and freedom of information to support staff in improving their overall awareness of information governance matters.

The Information Governance LearnPro training modules, are required to be completed every two years. The table below shows the number of staff members who have completed this training in the past 2 years.

Table 11.1: Compliance with information governance training

Clinical Boards	Previous two year total	**Current two year total**
Borders General Hospital Clinical Board	915	843
Chief Executive	17	11
Learning Disabilities	55	36
Mental Health Clinical Board	238	246
Primary and Community Services	528	507
Support Services	598	609
Grand Total	2351	**2252**

12 Patient Information

Health Rights Information Scotland is a project based within Consumer Focus Scotland which is funded by the Scottish Government Health Directorate. It is a joint initiative to raise the quality of information available to patients in the NHS. They produce information for patients about their rights, about how to use NHS services, and about what they can expect from the NHS, in particular issues of consent, making a complaint, confidentiality and patient records.

NHS Borders distributes these booklets widely across the organisation to make them available to the public. These are also published on the BISSY patient information systems installed at locations across the Borders and to our intranet and internet sites together with links to the Health Rights Information Scotland website.

13 Internal Audit Report 2015/16

An internal audit of Patients Records Management was carried out during 2015/16 and the report issued in October 2015.

The overall outcome was a grading of Low with the following risks identified:

1. Risk of breaching patient confidentiality and non-compliance with legislation if, when casenotes are out of the secure health records stores for extended periods, their location is not checked. Monitoring process to be reviewed.

   Current status: Complete – arrangements in place to introduce sample checking of casenote location.

2. Management information is not collected to support robust internal monitoring of SMR data accuracy received from clinicians.

Current status: Complete – information quality monitoring system now in place

3. TrakCare system biannual activity review Standard Operating Procedure lacks clarity to facilitate consistent application.

Current status: Complete – Standard Operating Procedure updated and procedures strengthened to ensure checks occur at the agreed frequency.

14 Best Value

To comply with the governance statement required by the Audit Committee as part of the Board's Annual Accounts process, the Information Governance Committee is required to make reference specifically to any work in year on best value completed by the committee.

The NHS Borders Best Value Framework "Use of Resources" theme focuses on how a Best Value organisation ensures that it makes effective, risk-aware and evidence-based decisions on the use of all of its resources stating. The information Governance committee is specifically responsible for ensuring, *"There is a robust information governance framework in place that ensures proper recording and transparency of all the organisation's activities and supports appropriate exploitation of the value of the organisation's information."*

In this year, the following work has supported the committee in meetings its obligations:

- Produce and submit a draft Records Management Plan to the Keeper of the Records of Scotland in compliance with the Public Records (Scotland) Act 2011
- Refining the Subject Access Request process to clarify the requirement for clinicians to authorise release of information, including performing any necessary redaction.
- Refining the Incident Summary report and providing copies of the reports, including the FairWarning report, to the various clinical boards/Support services
- Revised Internet policy approved
- Involvement in Lothian/Borders project to review the Pan Lothian/Borders Data Sharing Protocol
- Quarterly reporting of activity and performance for monitoring and recommendations by the committee of:
    - Data Access requests
    - Freedom of Information requests
    - Incident reports
    - E-learning modules completed
    - Confidentiality statements signed

15 Issues & challenges for 2016/17

Although most of the elements of work which make up information governance are well established within NHS Borders, the changing national standards and delivery of the Information Assurance Strategy for 2015-17 from the Scottish Government and implementation of the Records Management Plan will continue to provide a focus for developing these areas of the service.

15.1 The Public Records (Scotland) Act 2011

The Public Records Scotland Act, 2011 (PRSA) brings new standards of record management and accountability to the public sector with the aim of improving efficiency. Some elements have already been implemented, but the wider task of developing organisation wide plans and systems will require significant involvement of the information governance team in the coming year.

NHS Borders met the Keeper of the Records of Scotland's challenging deadline to deliver a draft Records Management Plan by January 2016. To date a response has not been received from the Keeper but when it is this will initiate the next phase: implementation. With no other resource currently identified it is likely that this work will continue to account for a significant part of the Information Governance team's workload, affecting the delivery of other elements on the Work Plan.

15.2 Raising awareness

During 2015/16 the Information Commissioner took enforcement action against several health organisations in the UK for breaching data protection. This action included one monetary penalty notice and nine Undertakings being issued. There were also two prosecutions of individuals who had accessed patient records inappropriately. The message is very clear, there will be no leniency shown for the public sector and organisations need to be confident that all staff members are provided with the knowledge and awareness to ensure standards can be maintained. Continued training and awareness will be required to maintain this message and safeguard personal information.

15.3 Incident reporting

Significant work has been done in this area resulting in only a modest increase in incident numbers. It remains a key priority on the IG Action Plan. Work will continue to ensure staff and managers are aware of what constitutes an information governance incident. There is also work to be done to further improve managers follow up of incidents. This is an organisation wide problem and does not just apply to information governance.

15.4 Resources

The addition of the Information Governance Officer post continues to make a significant positive impact on the workload. This post enables us to meet commitments within the eHealth strategy to strengthen IG arrangements and is funded non recurrently from eHealth Strategy allocations. Increasing focus on IG and therefore demands on the service to support NHS Borders discharge its obligations means that establishing recurring support for the continuation of this post will be a priority in the coming year.

Statement of Approval

This report has been produced in line with the NHS Borders Annual Accounts for the year ended 31 March 2016. The Information Governance Committee is a governance committee which reports to Borders NHS Board. This report provides assurance to Borders NHS Board that it is fulfilling its statutory obligations in the field of information governance.

Approved by: June Smyth, Executive Director for Information Governance

Signed (June Smyth) **Date**

Appendix 1: Information Governance Committee Membership

S MacDonald	Medical Director, Chair (until December 2015)
A Mordue	Consultant of Public Health, Caldicott Guardian, Chair (from January 2015)
E Rodger	Director of Nursing & Midwifery
J Stephen	Head of IM&T
G Ironside	Senior Health Information Manager
I Merritt	Information Governance Lead
J Dickson	Information Governance Officer
L Jones	Head of Healthcare Governance & Quality
H Clinkscale	Head of Training & Professional Development
J Laing	Operational Lead, Training & Professional Development
V Buchan	Senior Finance Manager
G Bouglas	Human Resources Manager
C Herbert	Head of Human Resources
K Liddington	Knowledge Management Coordinator

Appendix 2: Dates of Meetings and Attendees

09 June 2015

George Ironside	Senior Health Information Manager (Chair)
Alan Mordue	Caldicott Guardian
Dr Sheena MacDonald	Medical Director
Ian Merritt	Information Governance Lead
Kath Liddington	Knowledge Management Coordinator

In attendance:

Liz Lisle	Minutes
Carol Graham	Freedom of Information

08 September 2015

Dr Sheena MacDonald	Medical Director (Chair)
Alan Mordue	Caldicott Guardian
Jackie Stephen	Head of IM&T
Laura Jones	Clinical Governance Lead
George Ironside	Senior Health Information Manager
Janice Laing	(Deputising for Helen Clinkscale, Training & Development)
Viv Buchan	Finance
Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer

In attendance:

Liz Lisle	Minutes
Carol Graham	Freedom of Information

08 December 2015

Dr Sheena MacDonald	Medical Director (Chair for part of meeting)
Alan Mordue	Caldicott Guardian (Chair for part of meeting)
George Ironside	Senior Health Information Manager
Janice Laing	(Deputising for Helen Clinkscale, Training & Development)
Viv Buchan	Finance
John McLaren	Employee Director

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer
Carol Graham	Freedom of Information
Liz Lisle	Minutes
Jan Turnbull	Practice Education Facilitator (for 1 item)

08 March 2016

George Ironside	Senior Health Information Manager (Chair)
Jackie Stephen	Head of IM&T
Anne Palmer	(Deputising for Laura Jones, Clinical Governance)
Kim Carter	Senior Finance Manager

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer
Liz Lisle	Minutes

Appendix 3: Incident Categories

Subcategory 1 (Incident class)	**Subcategory 2 (Incident summary)**	**Examples (not exhaustive list)**
Breach of confidentiality	Permitted password to be used by other person	Gave a network or system password to another person and knowingly allowed them to access the system in their name.
	Confidential information found in public/inappropriate place	Information found in an insecure location and visible or potentially visible to unauthorised persons
	Confidential waste left insecure	Red bags and other confidential waste left in areas not designated as secure.
	Confidential information sent to wrong recipient	Information posted emailed or sent via any other means to wrong recipient.
	Confidential information emailed to inappropriate destination	Confidential information emailed with or without encryption, to an address or domain that should not receive it, e.g. home email address.
	Information divulged intentionally	Confidential information passed to unauthorised person by the spoken word, email, or any other means.
	Information divulged carelessly	Confidential information overheard in public place.
Failing to Secure	Hardcopy confidential/sensitive data lost/misplaced/stolen	Patient lists and/or other confidential documentation (printouts, hand written notes, diaries, etc.) lost, misplaced or stolen.
	Hardcopy confidential information sent using inappropriate method	Hardcopy confidential information sent in transit envelopes or not sealed or not sent via Special Delivery as appropriate.
	Confidential information sent but not received	Information sent but not received by recipient.
	Confidential information emailed without appropriate security	Confidential information emailed without encryption, or with identifiable data shown in subject line.
Inappropriate Access	Accessed own record (FW)	Person viewed own record.
	Accessed family member record (FW)	Person viewed record of family member who was not under the care or administration of that staff member.
	Accessed work colleague record (FW)	Person viewed record of work colleague who was not under the care or administration of that staff

Subcategory 1 (Incident class)	**Subcategory 2 (Incident summary)**	**Examples (not exhaustive list)**
		member.
	Accessed neighbour record (FW)	Person viewed record of neighbour who was not under the care or administration of that staff member.
	Accessed acquaintance/friend record (FW)	Person viewed record of friend, acquaintance or other person known to staff member who was not under the care or administration of that staff member.
	Accessed other person's record inappropriately (FW)	Person viewed record of patient who was not under the care or administration of that staff member. Would include High Profile person or person other than that listed in previous categories.
	Accessed Clinical records without due reason (Not FW)	Person viewed record of patient who was not under the care or administration of that staff member. Would normally refer to hard copy records or detected by means other than FairWarning.
	Used password of other person	Used the system access of another person to gain access, with or without the rightful owner's permission.
Incorrectly filed	Patient documents/labels found in wrong record	Notes belonging to one patient being found in the record of another.
	Patient documents/labels not filed at all or not in correct place in record	Notes left in folder flap and not filed correctly in record, or left separate from record completely.

NHS Borders

Information Governance Committee
Annual Report

2015/16

Contents

Introduction

This is the ninth NHS Borders Information Governance Annual Report, and covers the financial year 2015/16 to meet the Board's Governance Reporting cycle.

Information Governance is the framework within which we manage the information we hold as an organisation. The main principles aim to ensure that we handle information in a confidential and secure manner to appropriate ethical and quality standards. Information Governance covers all types of information and is the responsibility of all staff.

The work is underpinned by the following:

- The Data Protection Act 1998
- The Freedom of Information (Scotland) Act 2002
- The Public Records (Scotland) Act 2011
- Confidentiality: NHS Scotland Code of Practice
- Records Management
- Information Security Standard
- NHS Data Quality Assurance (Data Accreditation)
- Caldicott Guardianship

With the introduction of several public WiFi hotspots and social media for business use, revisions have been made to the Internet policy to reflect these. Enhancements were made to the Subject Access Process to reaffirm the health professionals' key role in authorising the release of personal information.

A new LearnPro module has been developed based on the Information Governance Code of Conduct. This is scheduled to be published over the next Quarter and is to further remind NHS Borders staff of information governance matters.

These are just some of the key achievements made over the year and we aim to improve the level of compliance with the Information Governance Standards by keeping our staff well informed about their responsibilities, and providing an effective governance structure within which to work.

Much of the year ahead will be taken up with implementing elements of the NHS Borders Records Management Plan that was developed during 2015/16 as specified under the Public Records (Scotland) Act 2011. In addition, there will be a significant amount of resource required to progress compliance with the NHS Scotland Information Assurance Strategy Framework.

June Smyth
Executive Director for Information Governance

1 Overview

Information Governance is a strategic framework to ensure guidance and best practice is applied to the way we handle information, as an organisation and as individual members of staff. Information governance encompasses the following work strands:

- Confidentiality
- Caldicott
- Data Quality Assurance
- Data Protection
- Freedom of Information
- Information Security
- Records Management
- Staff training and awareness

Information Governance covers all types of information and is the responsibility of all of NHS Borders staff, both clinical and non-clinical.

1.1 Information Governance Standards

The NHS Scotland Information Governance Standards were first published in November 2005 and monitored nationally until 2012 using a toolkit to assess the various elements.

In 2010/11, it was agreed that NHS Borders had achieved Level 2 for all ten standards in the Toolkit, with policies, procedures and training schedules in place. Since 2012, active monitoring against the toolkit has been discontinued. Progress has continued to be made through the Information Governance Work Plan.

No further work has taken place nationally to release a new toolkit. However, as part of the 2015 – 2017 Information Assurance Strategy, there is a new Information Assurance Framework. It is being proposed that this framework is used in place of a toolkit by all NHS Scotland organisations to demonstrate compliance and best practice.

1.2 Information Assurance Strategy

In November 2011, the Scottish Government first published a four year NHS Scotland Information Assurance (IA) Strategy which set out the strategic direction for further developing the IA capability and effectively embedding an IA culture across NHS Scotland.

The Strategy identified key outcomes and actions to be taken at a national and a local level to support the developments from the eHealth strategy. Most of the actions set out in the strategy at a national level were developed in consultation with health boards to support the eHealth Strategy. The actions have been mapped against what was in place within NHS Borders, to prioritise areas for attention.

With the 2015 – 2017 Information Assurance Strategy now released by the Scottish Government, the Information Governance direction of travel for the coming year and beyond has now been established for NHS Borders.

2 Structure

2.1 Information Governance Team

The Information Governance team was established in March 2009 and reports to the Information Governance Committee. It is managed by the Senior Health Information Manager and comprises the Information Governance Lead and the Information Governance Officer.

2.2 Information Governance Committee

The Committee met on four occasions in the year. The main business of the meetings has been carried out following a standing agenda incorporating the following elements:

- Information Governance Action Plan - exception reporting
- Information Governance Incident Reporting
- Freedom of Information
- Information Security
- Records Management and Data Quality
- Staff Awareness and Training
- Internal and external papers for consultation

Details of the Information Governance Committee membership are provided in Appendix 1, and meeting attendance in Appendix 2.

3 Policy & Planning

3.1 Records Management Strategy & Policy

Both the NHS Borders Records Management Strategy and Policy were reviewed in 2015 as part of Public Records (Scotland) Act work. The revised versions were approved by the Information Governance Committee in December 2015.

The Information Governance Policy has been revised to include reference to the Environmental Information Regulations. Compliance with the policy in terms of learning and signing confidentiality statements is now part of Clinical Board Performance Review Scorecard targets.

Key performance indicators were agreed by the IG Committee and continued to be reported on during 2015/16.

3.2 Information Governance Action Plan

Having moved away from the Information Governance toolkit, the IG Team have amalgamated the action plans for information assurance, records management, information security and information governance onto one work plan. Through this, the IG Team manage the work and provide exception reports to the Information Governance Committee.

Most of the year has been taken up with developing and producing the Records Management Plan as required by the Public Records (Scotland) Act 2011. The draft Plan was submitted to the Keeper of the Records of Scotland on time, at the end of January 2016. Acceptance of the Plan is expected from the Keeper during Q1/2 2016/17.

The IG team has also worked on a range of other issues during the year. These include:

- **Redeveloping the LearnPro training module** – This is based on the content of the Information Governance Code of Conduct, complementing the detail within that. It is scheduled to be published during Quarter 2 2016/17.
- **Updated the Information Governance Committee ToR –** Based on comments received by senior managers and discussions with other Boards the Terms of Reference for the Committee have been comprehensively revised with the Committee now reporting to the Clinical Executive Ops Group.

- Mobile Device Policy – Work continued on the development of a policy to define the use and security of "ultra" mobile devices, such as smartphones, tablets and similar products. This policy incorporates a "BYOD" element to cover personally owned devices. Local guidance is in place and has been issued to IT Services to follow when considering the introduction of any such devices to the organisation.
- Secure e-mail Guide – The Secure E-mail Guidance was updated following a move by the Scottish Government to change their e-mail domain to gov.scot. This was necessary to address the issue that mails to the new domain from NHS Mail addresses do not travel over a secure route and so were not approved for sensitive or confidential information
- Voice recognition devices – It was identified that the voice recognition devices used for dictation of patient notes were not configured in a way that was consistent with the NHS Scotland secure mobile data policy. Following discussions an agreement was reached to implement a unique PIN for each device and extend the timeout time period to 1 hour. These settings are now being applied to the entire estate.

3.3 Information Governance Code of Conduct for Staff

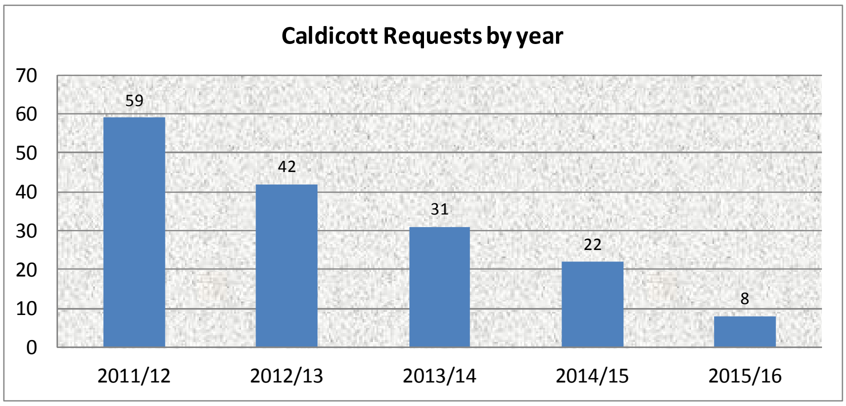
The NHS Borders Information Governance Code of Conduct for Staff, accompanied by new confidentiality statements and supported by an e-learning package, was formally launched in April 2011.

The Code was comprehensively revised during 2014/15 with a significant amount of work done to clarify the guidance on the removal of patient notes from Health Board premises. This covered instances where notes are needed in satellite clinics or patient homes, etc. The approval process for transporting notes was also simplified.

During 2015/16 the Information Governance team met with several different groups of staff, including GP staff, to deliver awareness training.

4 Caldicott Guardianship

Over the last year there were 8 applications for access to patient identifiable information which is a further significant drop on the previous year. This is largely due to requests being handled centrally by the Public Benefit and Privacy Panel which was set up by the Scottish Government and NHS Scotland. The Information Governance team lead is obliged to participate in these panels on two or three occasions per year with each attendance requiring a significant amount of work prior to the panel date.



Of these 8 requests, 3 were from IM&T staff wishing to access data. Other requests were concerned with audit (2), access by a relative (1) and other types of requests (2).

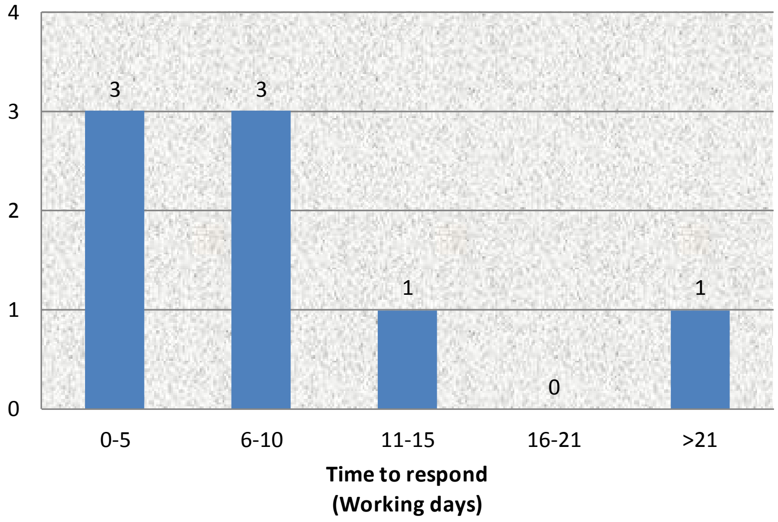
The table below shows that all 8 applications were approved, but only after conditions were applied or further safeguards to protect data security and confidentiality were agreed.

Table 4.1: Outcome of applications to the Caldicott Guardian, 2015/16

	Conditions specified		No Conditions specified		Total	
	Number	%	Number	%	Number	%
Approved	8	100%	0	0%	8	100%
Refused	0	0%	0	0%	0	0%
Total	8	100%	0	0%	**8**	100%

Generally applications that have conditions specified take longer to process as they need further investigation and scrutiny. Potentially this could contribute to the application going beyond the 15 working day target to process. The chart below shows performance against this target with all but one of the applications processed within 15 days, hitting the target.

Chart 4.1: Time to process Caldicott applications, 2015/16



5 Records Management

Public Records (Scotland) Act 2011

The work to address the requirements of the Public Records (Scotland) Act (PR(S)A) has dominated the Information Governance team's time over the past year.

Progress on the RMP to date includes:

- The formation of a Project Group that represents all areas of the organisation
- The creation of a Local Records Manager guidance document
- Completion of a Gap Analysis at a departmental level to establish the measures currently in place and to identify the areas each department will need to address to achieve corporate compliance
- Raising awareness of the fundamental changes to records management that the implementation of the RMP will impose

The current NHS Borders Records Management Policy sets out the principles of records management as well as schedules for maintaining, archiving and destruction of all types of records used by NHS Borders. This will be reviewed to ensure it meets the requirements of the Public Records (Scotland) Act 2011.

6 Subject Access Requests

Under the Data Protection Act, staff and patients (and their legal representatives) have the right to review the information which is held about them by an organisation. These requests are managed and monitored as “Subject Access Requests.”

The numbers of requests received by the Subject Access team continues to increase with a stepped increase around the time of the introduction of the Patient Rights Act Scotland 2011; as can be seen in chart 6.1.

Chart 6.1: Subject Access Requests by Category 2006/07 – 2015/16

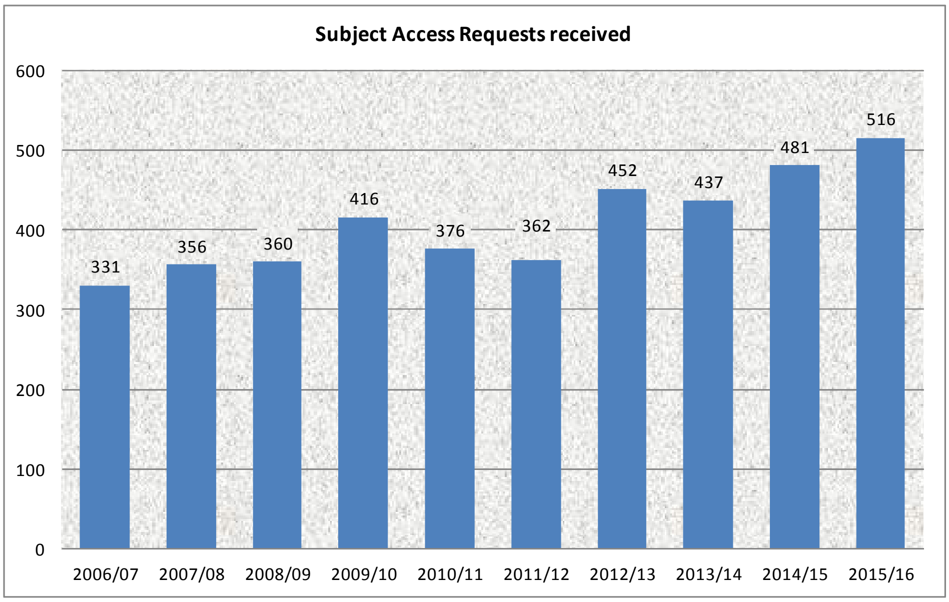


Chart 6.2: Subject Access Requests by Quarter 2015/16

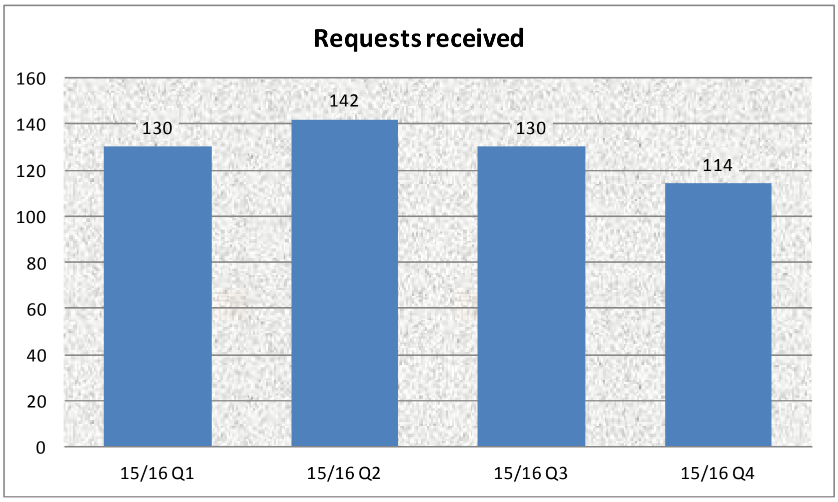
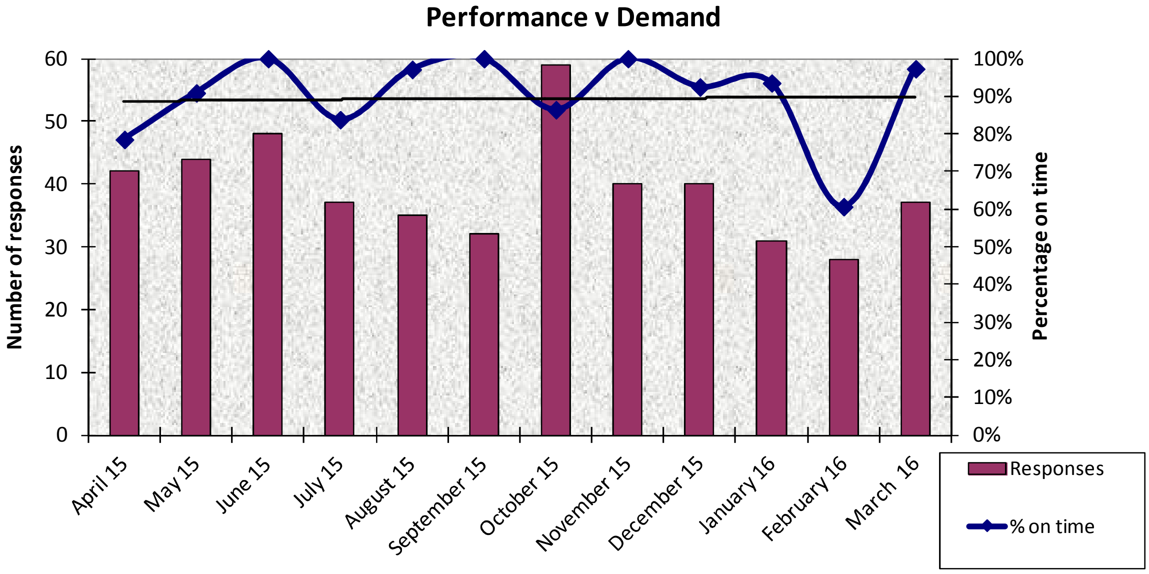


Chart 6.2: Subject Access Requests by Quarter 2015/16

Capacity within the Subject Access Request coordination team can impact on the ability to respond to all requests within the timescales stipulated by the Act. The chart below combines the number of requests responded to with the timescale compliance rate per month. Overall for the year, compliance was 90%.



7 Data Sharing

The Information Governance team was involved in reviewing the Pan Lothian/Borders Data Sharing Protocol. No changes were made to this document however Health and Social Care Integration will result in more data sharing agreements and procedures being developed over the next 12 months. It is likely that the Scottish Government preferred SASPI (Scottish Accord on the Sharing of Personal Information) model will be adopted in due course.

8 Information Security

As information technology has become essential in the management of information, it is necessary to ensure there are safeguards in place to enable information to be shared electronically with the right people without compromising confidentiality. This includes the accuracy and completeness of information, the safety of computer systems and software and preventing and minimizing the impact of system malfunctions.

Work has continued to formalise policies and protocols used within IM&T to ensure the systems run effectively across the organisation, and to ensure all staff are aware of their individual responsibilities for information security.

8.1 Standards and Guidance Documentation

Information Governance has a comprehensive library of standards, policies and guidance documents. Where appropriate, these are available on the Information Governance intranet page. During 2015/16 work continued to revise and update theses documents in accordance with good practice guidelines.

8.2 Mobile Computing

Progress has been made to pilot the use of handheld devices such as smartphones and tablets to support clinical care. It is important that information security be maintained with these, and the Information Governance team has developed technical security policies, in line with national guidelines, to ensure this is the case. This is a fast developing area and it is expected that ongoing work will be required in 2016/17.

8.3 Privacy Breach Detection Project

FairWarning remains the privacy breach detection tool used within NHS Borders and has now been in operation, providing daily reports, for 4 years.

The clinical information recording systems and patient management systems used within NHS Borders log the activity of users accessing the systems. FairWarning works by importing this information on a daily basis and collates reports according to predetermined categories, such as staff looking up their own records, or those of neighbours or family. These potential breaches of policy are checked to see whether the staff member is involved in the patient's care or administration. If not, they are forwarded to the appropriate line manager for further investigation.

The number of potential incidents (those where the predefined criteria were met) identified by FairWarning was down by 7% during 2015/16 on the previous year's figures. Of the 9,141 potential incidents only 132 cases were referred to line management for further investigation. This is up 11% on the previous year. As shown in the tables below, the number of confirmed incidents was also up: 12% higher than the previous year.

The increase in confirmed incidents has resulted in an awareness campaign being undertaken, with several communications issued via different methods through the year (Team Brief, Staff Update, Information Governance microsite, Featured Advert, etc.).

The breakdown of the confirmed incidents is shown in the tables below.

Table 8.1: Privacy breach detection investigations and outcomes

2012/13

Access Type	Amount
Self	82
Address	17
Family Member	23
Co-Worker	1
Total	**123**

2013/14

Access Type	Amount
Self	44
Address	4
Family Member	11
Co-Worker	1
Total	**60**

2014/15

Access Type	Amount
Self	29
Address	4
Family Member	5
High Profile	4
Co-Worker	2
Total	**44**

2015/16

Access Type	Amount
Self	40
Address	0
Family Member	3
High Profile	2
Co-Worker	5
Total	**50**

9 Incident Reporting

Breaches of data protection and information security are reported through Datix, the NHS Borders electronic incident reporting system. The system provides a record of the incident and the follow up actions and allows members of the Information Governance Team to track and follow up the actions taken. Each incident is investigated, and where appropriate, relevant action taken to address the specific issue. Generally this has involved providing additional education and awareness.

In November 2013 a major update to Datix was implemented and the opportunity was taken at this time to rationalise the Information Governance incident categories. This piece of work made it easier for incident reporters to select the correct category thus simplifying the summary reporting considerably. Appendix 3 shows the new categories and examples of incidents that fit each category.

The table below summarises the incidents reported over the past 12 months. The previous 2 years have also been included for comparison. While most incident categories have shown reduced numbers there was a 9% rise in the total number of reported incidents over the past 12 months. This is most due to a 38% increase in the number of staff viewing their own health records and an 18% increase in the reported cases of misfiling.

Table 9.1: Summary of Types of Incident

Incident class	Incident Summary	2013/14	2014/15	2015/16
Breach of Confidentiality	Confidential information emailed to inappropriate destination	5	1	6
	Confidential information found in public/inappropriate place	15	8	8
	Confidential information sent to wrong recipient	22	33	17
	Confidential waste left insecure	4	1	2
	Information divulged carelessly	7	2	6
	Information divulged intentionally	1	2	1
	Permitted password to be used by other person	1	2	1
Breach of Confidentiality Total		55	49	**41**
Failing to Secure	Confidential information emailed without appropriate security	0	1	1
	Confidential information sent but not received	2	1	2
	Hardcopy confidential information sent using inappropriate method	3	1	2
	Hardcopy confidential/sensitive data lost/misplaced/stolen	20	16	11
Failing to Secure Total		25	19	**16**
Inappropriate Access	Accessed acquaintance/friend record (FairWarning)	1	0	0
	Accessed clinical records without due reason (Not FW)	1	2	3
	Accessed family member record (FW)	6	2	2
	Accessed other person's record inappropriately (FW)	1	1	3
	Accessed own record (FW)	23	20	32
	Accessed work colleague record (FW)	0	3	4
	Used password of other person	1	1	0
Inappropriate Access Total		33	29	**44**
Incorrectly filed	Patient documents/labels found in wrong record	61	44	47
	Patient documents/labels not filed at all or not in correct place in record	5	2	9
Incorrectly filed Total		66	46	**56**
Grand Total		179	143	**157**

Table 9.2: Summary of Incident by Reporting Clinical Board

Clinical Board	2013/14	2014/15	2015/16
Acute	114	83	93
Learning Disabilities	1	2	1
Mental Health	13	4	19
Primary Care	19	13	16
Support Services	32	41	28
Grand Total	179	143	**157**

10 Freedom of Information

The Freedom of Information (Scotland) Act 2002 (FOISA) was introduced in January 2005. The Act requires all public authorities in Scotland to make any information they hold available on request. The FOI(S)A protocol is reviewed annually to ensure issues are addressed and to take account of developments in the FOI(S) system.

Each year since its introduction, there has been has been a steady increase in the number of requests. The majority of requests continue to relate to the performance of the NHS and particularly to the impact of Government cuts in funding and how this has impacted on Health Boards at a local level.

10.1 Activity

The volume of FOI requests slightly dipped with 2015/16 seeing a decrease of 0.5% on the previous year. Requests from the media continue to account for the highest volume of work at 37% with those from the Scottish Parliament accounting for 23%. The other categories have all roughly stayed the same.

10.2 Response Times

The Act requires that all requests are responded to within 20 working days. During the year 2015/16 our compliance slightly decreased to 98%.

The main reason for this decrease in compliance rate was the complexity of the FOI requests and the time it takes to secure final approval.

We continue to actively monitor and take action to ensure breaches are kept to a minimum and support departments to respond to requests within the required timescale. Wherever possible, the applicant is informed in advance of the likely delay and this helps to reduce the likelihood of the applicant complaining to the Scottish Information Commissioner.

Table 10.1: Compliance with statutory deadline

	2015/16	*2014/15*	*2013/14*	*2012/13*	*2011/12*	*2010/11*
Total number of requests responded to	503	527	331	399	326	331
Number of requests answered within 20 working days	497	524	243	325	292	298
Number of requests answered in more than 20 working days	6	3	88	74	34	33
Median number of days taken to respond	14	12	20	19	18	18
Percentage compliance	**98%**	**99%**	**74%**	**81%**	**90%**	**90%**

A full list of all the requests made to NHS Borders can be found on the Information Governance intranet site and on the NHS Borders website.

10.3 Reviews & appeals

Applicants who are unhappy with the response they receive or the way in which the response was handled may ask for a review of their request. If they remain dissatisfied, they may appeal to the Office of the Scottish Information Commissioner.

In 2015/16, eight applicants requested NHS Borders undertake an internal review of the handling of their request. Of these cases five responses were upheld and the other three were partially upheld.

There was one appeal to the Office of the Scottish Information Commissioner received in this time period. The Commissioner found NHS Borders had failed to comply with section 15(1) of FOISA (Duty to provide advice and assistance). Further details are available on the following link:

http://www.itspublicknowledge.info/ApplicationsandDecisions/Decisions/2015/201501218.aspx

10.4 Performance monitoring

Quarterly activity reports are produced for the Information Governance Committee. These reports detail the requests made, our response times for answering the requests and where exemptions are applied, among other performance indicators. These reports are published on the staff intranet and the NHS Borders website.

In order to comply with the spirit of the Act, it is important to ensure the use of exemptions is kept to a minimum. The default position is disclosure and when exemptions are considered, the risks and benefits are taken into account as part of the process. The most common reasons for not providing the applicant with the requested information are that it is already available elsewhere, usually on NHS Borders' or another organisation's website. The other main reason an exemption will be applied by NHS Borders is due to the fact we are a small Board and where the data relates to individual people, whether patients or staff we are bound by the Data Protection Act 1998 not to provide data on any statistic that is less than 5, therefore we are required to withhold under Section 38 of the FOISA. This is also in accordance with the Code of Practice for Official Statistics any number that is less than five, actual numbers and potentially identifiable information is withheld to help maintain patient confidentiality due to potential risk of disclosure. Further information is available in the ISD Statistical Disclosure Control Protocol.

Table 10.2: Outcome of requests

	2015/16	***2014/15***	***2013/14***	***2012/13***	***2011/12***	***2010/11***
All information released	***222***	***202***	200	190	165	188
Information part released	***206***	***152***	84	137	115	107
Information not held	***109***	***83***	67	122	19	77
Information withheld – cost of compliance	***27***	***31***	41	83	40	31
Exemptions applied	***139***	***90***	22	46	27	26
Vexatious request	***0***	***0***	0	0	0	0
Other (further clarification requested and not provided, invalid request, request withdrawn, redirected)	***9***	***7***	9	10	11	2

Note: some responses fall into more than one category

11 Training & Awareness

Training and awareness remains key to successful information governance within any organisation, as much of the national guidance and legislation for information governance is of a technical and detailed nature. Whilst improved IT solutions continue to be put in place, the success of these is in part dependant on staff compliance, and for compliance, staff need to be fully aware of their information governance responsibilities.

In 2015/16, in addition to a number of articles on information governance published in the Corporate Team Brief, Staff Update and IM&T Bulletin, emails have been issued widely across NHS Borders to highlight specific hot topics and the desktop "post-it" and Intranet Featured Advert have been utilised several times.

11.1 eLearning

All NHS Borders staff members are required to be fully familiar with the concepts and principles of information governance. As well as providing face to face training and awareness sessions, an e-learning package is available as part of the suite of mandatory training provided to staff. It includes basic learning in data security, confidentiality and freedom of information to support staff in improving their overall awareness of information governance matters.

The Information Governance LearnPro training modules, are required to be completed every two years. The table below shows the number of staff members who have completed this training in the past 2 years.

Table 11.1: Compliance with information governance training

Clinical Boards	Previous two year total	**Current two year total**
Borders General Hospital Clinical Board	915	843
Chief Executive	17	11
Learning Disabilities	55	36
Mental Health Clinical Board	238	246
Primary and Community Services	528	507
Support Services	598	609
Grand Total	2351	**2252**

12 Patient Information

Health Rights Information Scotland is a project based within Consumer Focus Scotland which is funded by the Scottish Government Health Directorate. It is a joint initiative to raise the quality of information available to patients in the NHS. They produce information for patients about their rights, about how to use NHS services, and about what they can expect from the NHS, in particular issues of consent, making a complaint, confidentiality and patient records.

NHS Borders distributes these booklets widely across the organisation to make them available to the public. These are also published on the BISSY patient information systems installed at locations across the Borders and to our intranet and internet sites together with links to the Health Rights Information Scotland website.

13 Internal Audit Report 2015/16

An internal audit of Patients Records Management was carried out during 2015/16 and the report issued in October 2015.

The overall outcome was a grading of Low with the following risks identified:

1. Risk of breaching patient confidentiality and non-compliance with legislation if, when casenotes are out of the secure health records stores for extended periods, their location is not checked. Monitoring process to be reviewed.

   Current status: Complete – arrangements in place to introduce sample checking of casenote location.

2. Management information is not collected to support robust internal monitoring of SMR data accuracy received from clinicians.

   Current status: Complete – information quality monitoring system now in place

3. TrakCare system biannual activity review Standard Operating Procedure lacks clarity to facilitate consistent application.

   Current status: Complete – Standard Operating Procedure updated and procedures strengthened to ensure checks occur at the agreed frequency.

14 Best Value

To comply with the governance statement required by the Audit Committee as part of the Board's Annual Accounts process, the Information Governance Committee is required to make reference specifically to any work in year on best value completed by the committee.

The NHS Borders Best Value Framework "Use of Resources" theme focuses on how a Best Value organisation ensures that it makes effective, risk-aware and evidence-based decisions on the use of all of its resources stating. The information Governance committee is specifically responsible for ensuring, *"There is a robust information governance framework in place that ensures proper recording and transparency of all the organisation's activities and supports appropriate exploitation of the value of the organisation's information."*

In this year, the following work has supported the committee in meetings its obligations:

- Produce and submit a draft Records Management Plan to the Keeper of the Records of Scotland in compliance with the Public Records (Scotland) Act 2011
- Refining the Subject Access Request process to clarify the requirement for clinicians to authorise release of information, including performing any necessary redaction.
- Refining the Incident Summary report and providing copies of the reports, including the FairWarning report, to the various clinical boards/Support services
- Revised Internet policy approved
- Involvement in Lothian/Borders project to review the Pan Lothian/Borders Data Sharing Protocol
- Quarterly reporting of activity and performance for monitoring and recommendations by the committee of:
  - Data Access requests
  - Freedom of Information requests
  - Incident reports
  - E-learning modules completed
  - Confidentiality statements signed

15 Issues & challenges for 2016/17

Although most of the elements of work which make up information governance are well established within NHS Borders, the changing national standards and delivery of the Information Assurance Strategy for 2015-17 from the Scottish Government and implementation of the Records Management Plan will continue to provide a focus for developing these areas of the service.

15.1 The Public Records (Scotland) Act 2011

The Public Records Scotland Act, 2011 (PRSA) brings new standards of record management and accountability to the public sector with the aim of improving efficiency. Some elements have already been implemented, but the wider task of developing organisation wide plans and systems will require significant involvement of the information governance team in the coming year.

NHS Borders met the Keeper of the Records of Scotland's challenging deadline to deliver a draft Records Management Plan by January 2016. To date a response has not been received from the Keeper but when it is this will initiate the next phase: implementation. With no other resource currently identified it is likely that this work will continue to account for a significant part of the Information Governance team's workload, affecting the delivery of other elements on the Work Plan.

15.2 Raising awareness

During 2015/16 the Information Commissioner took enforcement action against several health organisations in the UK for breaching data protection. This action included one monetary penalty notice and nine Undertakings being issued. There were also two prosecutions of individuals who had accessed patient records inappropriately. The message is very clear, there will be no leniency shown for the public sector and organisations need to be confident that all staff members are provided with the knowledge and awareness to ensure standards can be maintained. Continued training and awareness will be required to maintain this message and safeguard personal information.

15.3 Incident reporting

Significant work has been done in this area resulting in only a modest increase in incident numbers. It remains a key priority on the IG Action Plan. Work will continue to ensure staff and managers are aware of what constitutes an information governance incident. There is also work to be done to further improve managers follow up of incidents. This is an organisation wide problem and does not just apply to information governance.

15.4 Resources

The addition of the Information Governance Officer post continues to make a significant positive impact on the workload. This post enables us to meet commitments within the eHealth strategy to strengthen IG arrangements and is funded non recurrently from eHealth Strategy allocations. Increasing focus on IG and therefore demands on the service to support NHS Borders discharge its obligations means that establishing recurring support for the continuation of this post will be a priority in the coming year.

Statement of Approval

This report has been produced in line with the NHS Borders Annual Accounts for the year ended 31 March 2016. The Information Governance Committee is a governance committee which reports to Borders NHS Board. This report provides assurance to Borders NHS Board that it is fulfilling its statutory obligations in the field of information governance.

Approved by: June Smyth, Executive Director for Information Governance

Signed (June Smyth) **Date**

Appendix 1: Information Governance Committee Membership

S MacDonald	Medical Director, Chair (until December 2015)
A Mordue	Consultant of Public Health, Caldicott Guardian, Chair (from January 2015)
E Rodger	Director of Nursing & Midwifery
J Stephen	Head of IM&T
G Ironside	Senior Health Information Manager
I Merritt	Information Governance Lead
J Dickson	Information Governance Officer
L Jones	Head of Healthcare Governance & Quality
H Clinkscale	Head of Training & Professional Development
J Laing	Operational Lead, Training & Professional Development
V Buchan	Senior Finance Manager
G Bouglas	Human Resources Manager
C Herbert	Head of Human Resources
K Liddington	Knowledge Management Coordinator

Appendix 2: Dates of Meetings and Attendees

09 June 2015

George Ironside	Senior Health Information Manager (Chair)
Alan Mordue	Caldicott Guardian
Dr Sheena MacDonald	Medical Director
Ian Merritt	Information Governance Lead
Kath Liddington	Knowledge Management Coordinator

In attendance:

Liz Lisle	Minutes
Carol Graham	Freedom of Information

08 September 2015

Dr Sheena MacDonald	Medical Director (Chair)
Alan Mordue	Caldicott Guardian
Jackie Stephen	Head of IM&T
Laura Jones	Clinical Governance Lead
George Ironside	Senior Health Information Manager
Janice Laing	(Deputising for Helen Clinkscale, Training & Development)
Viv Buchan	Finance
Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer

In attendance:

Liz Lisle	Minutes
Carol Graham	Freedom of Information

08 December 2015

Dr Sheena MacDonald	Medical Director (Chair for part of meeting)
Alan Mordue	Caldicott Guardian (Chair for part of meeting)
George Ironside	Senior Health Information Manager
Janice Laing	(Deputising for Helen Clinkscale, Training & Development)
Viv Buchan	Finance
John McLaren	Employee Director

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer
Carol Graham	Freedom of Information
Liz Lisle	Minutes
Jan Turnbull	Practice Education Facilitator (for 1 item)

08 March 2016

George Ironside	Senior Health Information Manager (Chair)
Jackie Stephen	Head of IM&T
Anne Palmer	(Deputising for Laura Jones, Clinical Governance)
Kim Carter	Senior Finance Manager

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer
Liz Lisle	Minutes

Appendix 3: Incident Categories

Subcategory 1 (Incident class)	**Subcategory 2 (Incident summary)**	**Examples (not exhaustive list)**
Breach of confidentiality	Permitted password to be used by other person	Gave a network or system password to another person and knowingly allowed them to access the system in their name.
	Confidential information found in public/inappropriate place	Information found in an insecure location and visible or potentially visible to unauthorised persons
	Confidential waste left insecure	Red bags and other confidential waste left in areas not designated as secure.
	Confidential information sent to wrong recipient	Information posted emailed or sent via any other means to wrong recipient.
	Confidential information emailed to inappropriate destination	Confidential information emailed with or without encryption, to an address or domain that should not receive it, e.g. home email address.
	Information divulged intentionally	Confidential information passed to unauthorised person by the spoken word, email, or any other means.
	Information divulged carelessly	Confidential information overheard in public place.
Failing to Secure	Hardcopy confidential/sensitive data lost/misplaced/stolen	Patient lists and/or other confidential documentation (printouts, hand written notes, diaries, etc.) lost, misplaced or stolen.
	Hardcopy confidential information sent using inappropriate method	Hardcopy confidential information sent in transit envelopes or not sealed or not sent via Special Delivery as appropriate.
	Confidential information sent but not received	Information sent but not received by recipient.
	Confidential information emailed without appropriate security	Confidential information emailed without encryption, or with identifiable data shown in subject line.
Inappropriate Access	Accessed own record (FW)	Person viewed own record.
	Accessed family member record (FW)	Person viewed record of family member who was not under the care or administration of that staff member.
	Accessed work colleague record (FW)	Person viewed record of work colleague who was not under the care or administration of that staff

Subcategory 1 (Incident class)	Subcategory 2 (Incident summary)	Examples (not exhaustive list)
		member.
	Accessed neighbour record (FW)	Person viewed record of neighbour who was not under the care or administration of that staff member.
	Accessed acquaintance/friend record (FW)	Person viewed record of friend, acquaintance or other person known to staff member who was not under the care or administration of that staff member.
	Accessed other person's record inappropriately (FW)	Person viewed record of patient who was not under the care or administration of that staff member. Would include High Profile person or person other than that listed in previous categories.
	Accessed Clinical records without due reason (Not FW)	Person viewed record of patient who was not under the care or administration of that staff member. Would normally refer to hard copy records or detected by means other than FairWarning.
	Used password of other person	Used the system access of another person to gain access, with or without the rightful owner's permission.
Incorrectly filed	Patient documents/labels found in wrong record	Notes belonging to one patient being found in the record of another.
	Patient documents/labels not filed at all or not in correct place in record	Notes left in folder flap and not filed correctly in record, or left separate from record completely.