Information Governance Committee Annual Report

2019/20

Contents

Introduction

This is the thirteenth NHS Borders Information Governance Annual Report and covers the financial year 2019/20 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 General Data Protection Regulation 2016
- The Data Protection Act 2018
- 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

The past 12 months has largely been concerned with moving towards a more compliant position with regards the General Data Protection Regulation (GDPR). The Information Governance team have worked with various teams and departments to increase the number of Information Asset Register returns submitted by the organisation. Work will continue on this over the coming year. The overall impact of the Covid 19 pandemic is yet to be fully realised but the focus for much of NHS Borders has shifted during the last quarter of this financial year.

Work has been undertaken to streamline the Information Governance requirements that all projects and developments must consider when processing personal information. A simple "one stop shop" has been introduced and published on the Information Governance microsite (http://intranet/resource.asp?uid=37655) that guides staff through the necessary process.

As in previous years the team has continued to publish "Featured Adverts" on the Intranet providing hints and tips to all staff about keeping them and NHS Borders secure.

These are some of the key achievements made over the year and we aim to improve the level of compliance with Information Governance standards by keeping our staff well informed about their responsibilities, and providing an effective information governance structure within which to work. It is expected that much of the year ahead will continue to consolidate improvements in information handling that came with GDPR, and continued involvement in the local implementation of the Cyber Resilience Plan issued by Scottish Government eHealth Division. NHS Boards in Scotland have been asked to follow the Information Security Policy Framework (ISPF) until further development on the Scottish Public Sector Cyber Resilience Framework (CRF) has been completed.

Cliff Sharp
NHS Border Medical Director
Chair of Information Governance Committee

1 Overview

Information Governance provides a 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 Assurance Strategy

Scotland's Digital Health Care Strategy[1], in particular Domain B, and the Health and Social Care Information Sharing Strategy 2014-2020[2] are used as the basis to prioritise the rolling Information Governance work plan.

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. Work is ongoing to assess any changes necessary for the team required for them to meet the additional demands from the Data Protection Act 2018 and Cyber Resilience Framework.

2.2 Information Governance Committee

The Committee physically met on three of the planned four occasions in the year, the fourth being cancelled due to the Covid-19 pandemic. 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 and Cyber 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.

[1] https://www.digihealthcare.scot/wp-content/uploads/2018/04/25-April-2018-SCOTLANDS-DIGITAL-HEALTH-AND-CARE-STRATEGY-published.pdf
[2] https://www.gov.scot/publications/health-social-care-information-sharing-strategic-framework-2014-2020/pages/8/

2.3 Cyber Security group

The Cyber Security Group's purpose is to provide operational level guidance and monitoring on cyber security issues and to report performance, compliance and relevant issues to the Information Governance Committee. The Information Governance Lead and the Senior Health Information manager are members of the Cyber Security Group.

A requirement of the Scottish Government's Cyber Resilience Plan is for all Public Authorities in Scotland to gain Cyber Essentials certification. Cyber Essentials is a self assessment of the organisation's basic security controls that will protect against a wide variety of the most common cyber attacks.

The planned Cyber Essentials certification has not yet been achieved. This is due mainly to the number of unsupported Windows XP computers still necessarily on the network. These are required to run clinical systems that do not themselves support a later operating system. An ongoing project is expected to see the removal of these devices during 2020. A further complication now is the end of support for the Windows 7 operating system in January 2020. NSS have negotiated a support extension with Microsoft but this was not available to NHS Borders until March 2020.

In May 2018 the Network and Information Systems Regulations (2018) (NIS) passed into UK law. NIS places a legislative obligation on Operators of Essential Services (OESs). Scotland has 2 OESs (Scottish Water and NHS Scotland). All Scottish NHS Boards will be audited on NIS compliance over the course of 2020. This will be conducted by an independent auditor appointed by the Scottish Health Competent Authority (SHCA). Failure to meet NIS standards could in serious cases result in a financial penalty of up to £17M.

3 Policy & Planning

3.1 Records Management Policy

The Records Management Policy was reviewed by the Information Governance Lead and no changes were considered necessary.

3.2 Information Governance Policy

The Information Governance Policy (2018) incorporated minor updates relating to GDPR. Compliance with the policy in terms of learning and signing confidentiality statements continues to be monitored through performance scorecards.

3.3 Information Governance Action Plan

The IG Team have amalgamated the separate action plans for information assurance, records management, information security and information governance onto a single work plan. Through this, the IG Team manage the work and provides exception reports to the Information Governance Committee.

The Information Asset Register was introduced in 2018 as an additional requirement of GDPR and at that time all sections of the organisation were approached to populate it with details of their information assets. Progress on its completion has been slow but over the past 12 months the Information Governance team have been actively following up with departments to encourage completeness.

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

- **Create a "One stop shop" for Projects** – This process flow includes all necessary documentation that must be considered before processing personal information.
- **Introducing a charging scheme for Solicitor requests for personal information** – This applies to requests from solicitors that are not a Subject Access Request and do not fall under the normal SAR terms of the GDPR and can thus be charged for.

- **Producing Data Processing Agreements and Data Protection Impact Assessments** – have been produced for several projects including:
    - Counterweight
    - MacMillan Care Holistic Needs Assessment
    - Silvercloud Psychology system
    - Pharmacy Clozaril recording
    - Lothian Flow Centre
    - Office 365
    - TrakCare upgrade

3.4 Information Governance Staff Code of Conduct

The NHS Borders Information Governance Code of Conduct for Staff, first published in 2011, remains current and up to date. No changes have been required over the past 12 months.

4 Caldicott Guardianship

Over the last year there were 22 applications for access to patient identifiable information which is a decrease of 27% on the previous year. Most requests (95%) were from NHS Borders staff requesting access to patient records for new clinical systems such as BadgerNet and EMIS Community Web.

With the exception of the requests from NHS Borders there has been a significant drop in requests from other sources. 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 participates in these panels on three or four occasions per year. Each attendance requires a significant amount of preparatory work prior to the panel date.

Table 4.1: Outcome of applications to the Caldicott Guardian, 2019/20

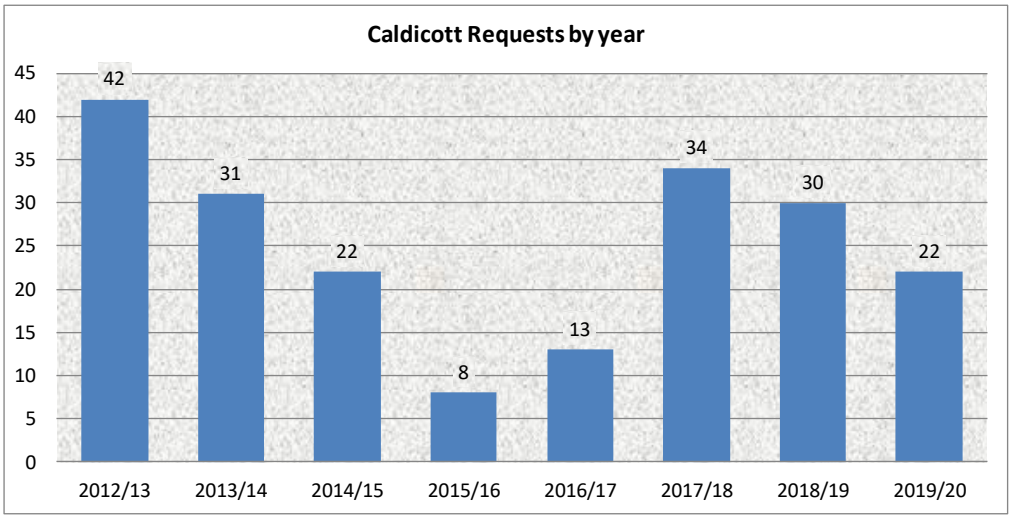
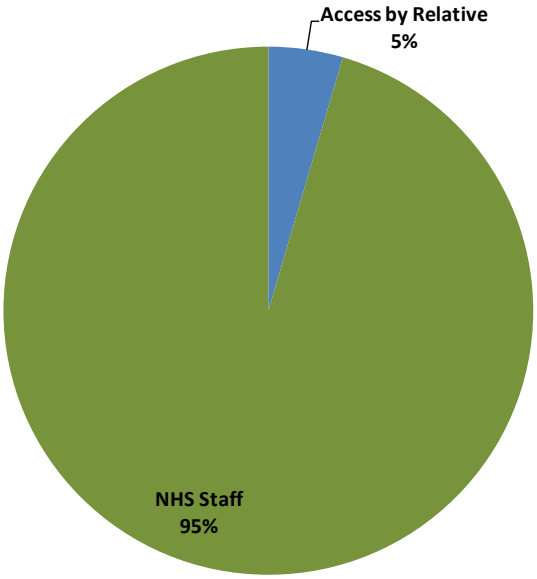


Table 4.2: Types of applications received by the Caldicott Guardian, 2019/20

The graph and table below show the spread of originators of the requests.

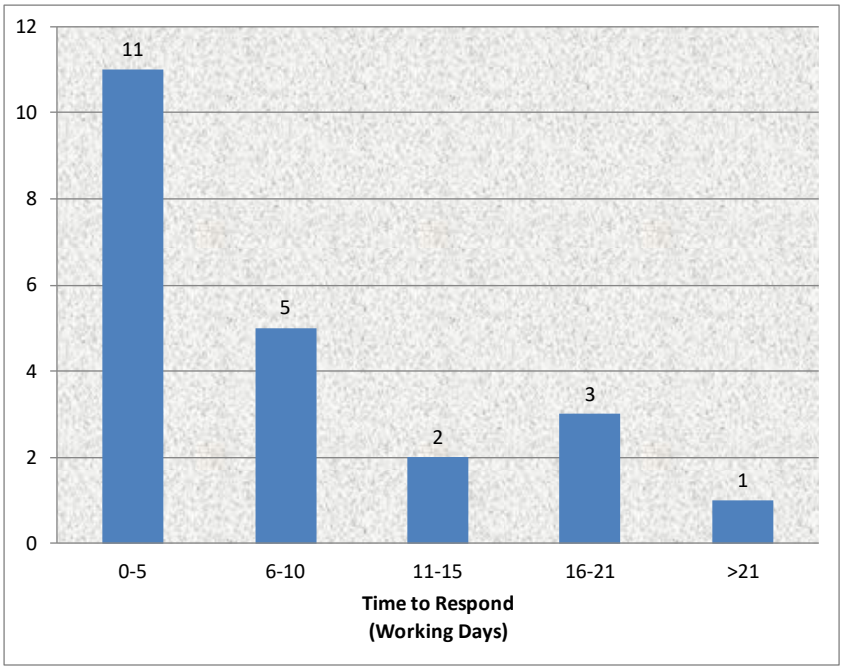


Application type	Number
Audit	
Research	
NHS Staff	21
Information Governance	
IM&T	
Access by Relative	1
Other	
Total	**22**

All applications were approved and no conditions were required to be applied or further safeguards to protect data security and confidentiality were necessary.

The chart below shows performance against the target of the 15 working days to process, with 82% meeting the target.

Chart 4.3: Time to process Caldicott applications, 2019/20



5 Records Management

Public Records (Scotland) Act 2011

Progress on the 2016 Records Management Plan (RMP) remains limited. It is planned that this work be progressed during 2020/21.

The elements relating to a standardised document naming convention and document storage should be addressed by the migration to Office 365 and the adoption of a national template for SharePoint.

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. The policy was reviewed during 2017/18 to ensure it continues to meet the requirements of the Public Records (Scotland) Act 2011. No further amendments have been made as a new national Records Management Policy, delayed in 2019, is expected to be published during 2020.

6 Subject Access Requests

Under Data Protection legislation (GDPR and DPA), 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 over the last 12 months continues to increase, in line with predictions, following the introduction of the General Data Protection Regulation in May 2018. Requests are up by 10% on the previous 12 months.

Under previous legislation, the existence of a charge of up to £50 resulted in around 15% of requesters withdrawing their request, thus reducing the amount of work required to be completed by the Subject Access team. There is not a similar provision in the Data Protection Act 2018: all requests received must now be fully complied with, resulting in additional work for the Subject Access team and the clinicians who must review the information before authorising it for release.

Chart 6.1: Subject Access Requests by Year 2007/08 – 2019/20

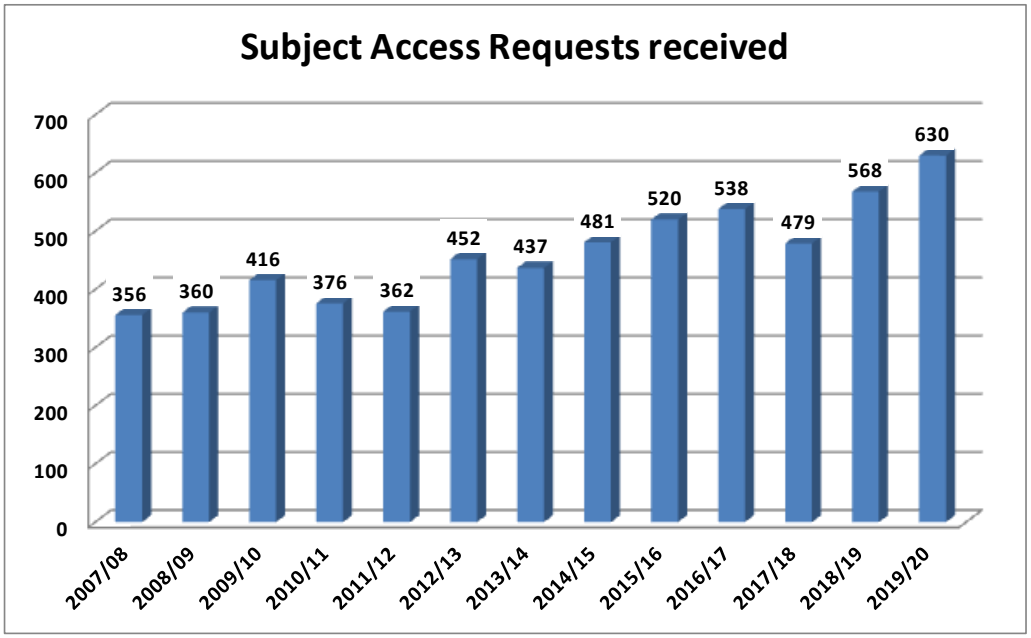


Chart 6.2: Subject Access Requests by Quarter 2019/20

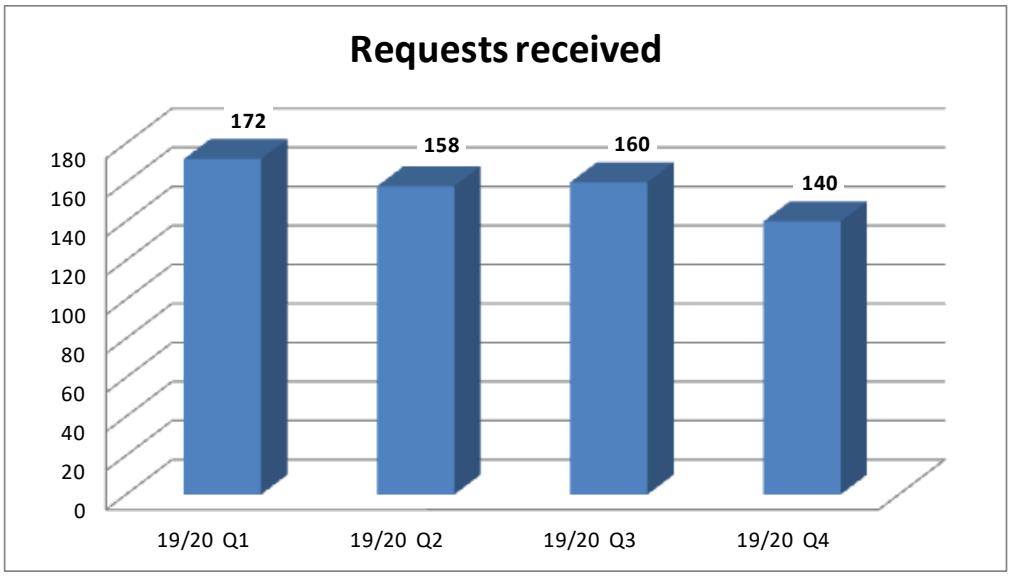
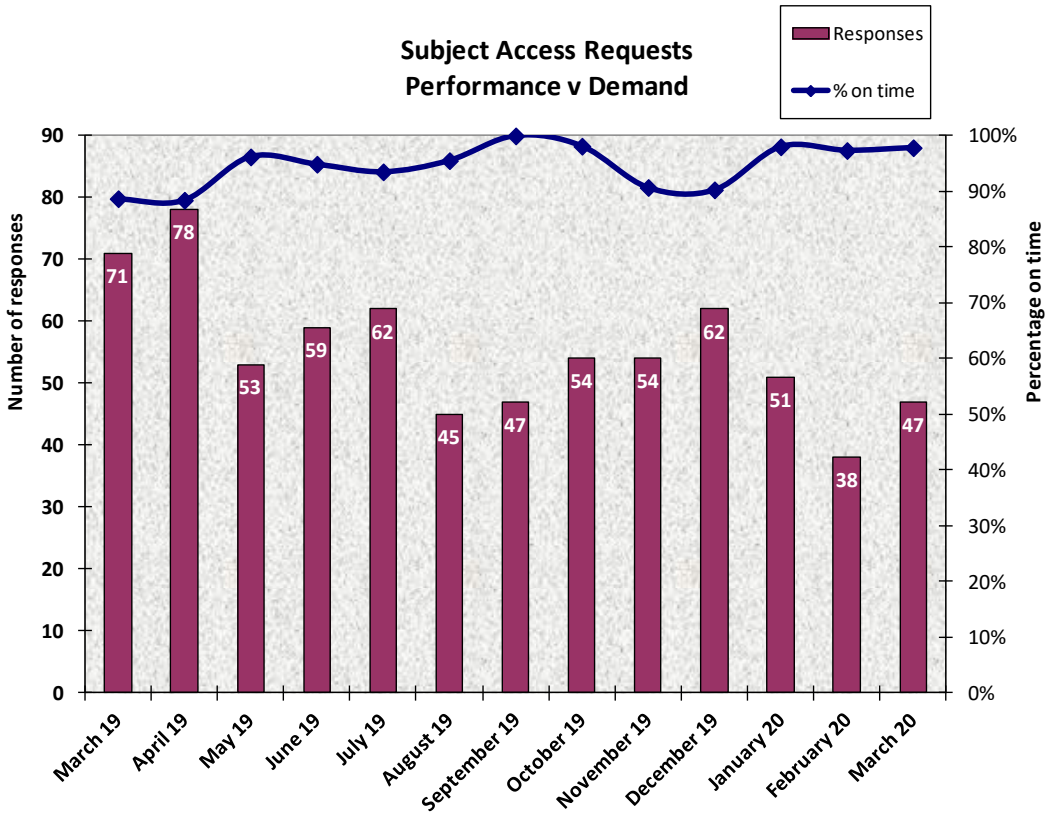


Chart 6.2: Subject Access Requests by Quarter 2019/20

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 following chart combines the number of requests responded to with the timescale compliance rate per month.



Overall compliance for the year was 95%, an improvement from 91% for the previous 12 months.

In total, 34 requests were responded to beyond the permitted one month time scale. The causes for the delay were:

Delay in receiving authorisation from clinician	41%
CD Burner failure (Radiology images)	26%
Patient notes required for clinic or inpatient	6%
Notes returned late to Medical Records	18%
Medical Records staff shortage	9%

7 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 continues to review and update the raft of policies and protocols relating to information used to ensure that IT systems run effectively across the organisation, and to ensure staff are aware of their individual responsibilities for information security.

7.1 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 2019/20 work continued to revise and update these documents in accordance with good practice guidelines.

In addition to other guidance documentation such as the user guide for the Information Asset Register, updated versions of Information Governance Code of Conduct, E-Mail Policy and the Data Protection policy have been published to reflect the General Data Protection Regulation.

7.2 Privacy Breach Detection Project

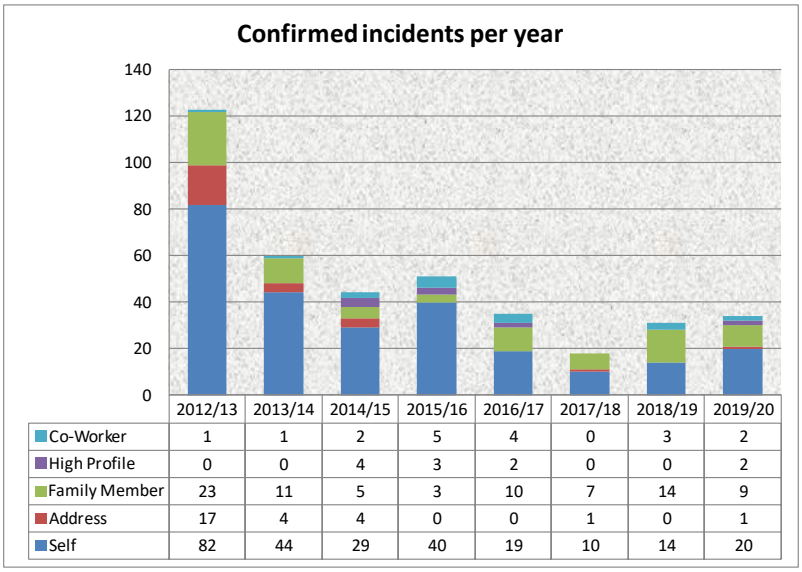
FairWarning remains the privacy breach detection tool used within NHS Borders and has been in operation since 2012.

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 up by 15% during 2019/20 on the previous year. Of the 12,245 potential incidents 160 cases were referred to line management for further investigation. This is also up 15% on the previous year. As shown in the tables below, the number of confirmed incidents had a small increase, of 6%, on the previous year to 34. Although the numbers of confirmed incidents has increased over the last 12 months, the overall trend since FairWarning was introduced is significantly down.

The breakdown of the confirmed incidents is shown in the chart and table below.

Chart 7.1: Privacy breach detection investigations and outcomes



	2012/13	2013/14	2014/15	2015/16	2016/17	2017/18	2018/19	2019/20
Co-Worker	1	1	2	5	4	0	3	2
High Profile	0	0	4	3	2	0	0	2
Family Member	23	11	5	3	10	7	14	9
Address	17	4	4	0	0	1	0	1
Self	82	44	29	40	19	10	14	20

8 Incident Reporting

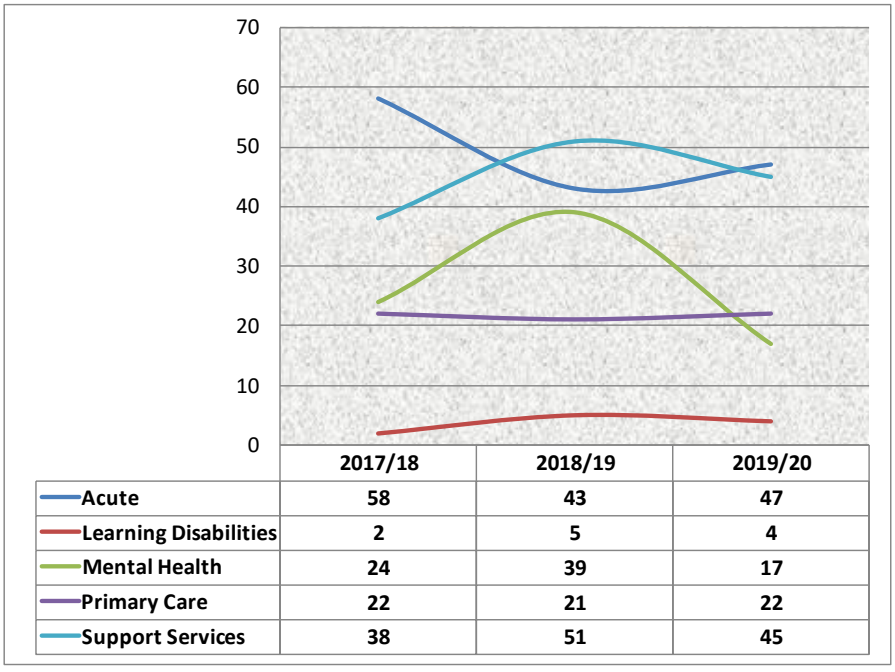
Breaches of data protection and information security are reported through Datix, the NHS Borders electronic incident reporting system. The system provides a record of the incident and the follow up actions and allows members of the Information Governance Team to track and follow up the actions taken.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

The tables below summarise the incidents reported over the past 12 months. There has been a 15% decrease in the number of incidents reported (135) compared with the previous year (159). Carelessness/human error continues to be the root cause of the majority of incidents with confidential information being sent to or left in inappropriate locations.

Table 8.1: Summary of Types of Incident

Incident class	Incident Summary	2017/18	2018/19	**2019/20**
Breach of Confidentiality	Confidential information emailed to inappropriate destination	19	25	14
	Confidential information found in public/inappropriate place	32	15	13
	Confidential information sent to wrong recipient	22	25	23
	Confidential waste left insecure	8	2	1
	Information divulged carelessly	0	9	11
	Information divulged intentionally	0	4	1
	Permitted password to be used by other person	0	0	0
Breach of Confidentiality Total		**81**	**80**	**63**
Failing to Secure	Confidential information emailed without appropriate security	1	1	2
	Confidential information sent but not received	1	2	0
	Hardcopy confidential information sent using inappropriate method	2	0	1
	Hardcopy confidential/sensitive data lost/misplaced/stolen	18	20	14
Failing to Secure Total		**22**	**23**	**17**
Inappropriate Access	Accessed acquaintance/friend record (FW)	1	1	0
	Accessed clinical records without due reason (Not FW)	0	4	2
	Accessed family member record (FW)	5	5	8
	Accessed neighbour record (FW)	0	0	0
	Accessed other person's record inappropriately (FW)	0	0	1
	Accessed own record (FW)	10	11	14
	Accessed work colleague record (FW)	0	3	2
	Used password of other person	0	0	1
Inappropriate Access Total		**16**	**24**	**28**
Incorrectly filed	Patient documents/labels found in wrong record	22	29	27
	Patient documents/labels not filed at all or not in correct place in record	3	3	0
Incorrectly filed Total		**25**	**32**	**27**
Grand Total		**144**	**159**	**135**

Table 8.2: Summary of Incidents by reporting Clinical Board



	2017/18	2018/19	2019/20
Acute	58	43	47
Learning Disabilities	2	5	4
Mental Health	24	39	17
Primary Care	22	21	22
Support Services	38	51	45

9 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 take account of developments in the FOI(S) system.

Each year since its introduction, there has been an increase in the number of requests but in this unprecedented year we have seen a decrease in requests due to Brexit and then the Coronavirus Covid 19 Pandemic. The majority of requests that were received continue to relate to the performance and expenditure of the NHS.

9.1 Activity

The volume of FOI requests decreased with 2019/20 seeing a decrease of 9% on the previous year. Requests from the Commercial sector now account for the highest volume of work at 27% with those from the Media sector at 22%. Requests from the Scottish Parliament dropped to 15% of the total number of request received but this was mainly due to Brexit. The other categories have all roughly stayed the same.

9.2 Response Times

The Act requires that all requests are responded to within 20 working days. During the year 2019/20 our compliance decreased to an average of 94%. The main reason behind this breach in compliance was the Coronavirus Pandemic when resources were aimed at managing the outbreak and supporting frontline operations and staff. Another factor in this drop in compliance was due to the FOI Coordinator role being reduced on a temporary basis to allow for a secondment opportunity.

The complexity, and sometimes sensitivity, of the FOI requests received can make achieving this compliance rate a challenge.

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, in the case of the Coronavirus Pandemic, prior to the introduction of emergency legislation where the timescales were amended from 20 to 60 working days, we published updates on our public website informing applicants of the reasoning behind the delays.

Table 9.1: Compliance with statutory deadline

	2019/20	*2018/19*	*2017/18*	*2016/17*	*2015/16*
Total number of requests responded to	**566**	622	617	623	527
Number of requests answered within 20 working days	**533**	616	594	619	524
Number of requests answered in more than 20 working days	**16**	6	23	4	3
Median number of days taken to respond	**10**	11	12	14	12
Percentage compliance	**94%**	99%	96%	99%	99%

* 17 FOI requests still outstanding at time of report

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.

9.3 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 2019/20 we received 4 requests for review; therefore there were no appeals to the Office of the Scottish Information Commissioner received in this time period.

9.4 Performance monitoring

Quarterly activity reports are provided to 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 2018 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 9.2: Outcome of requests

	2019/20	*2018/19*	*2017/18*	*2016/17*	*2015/16*
All information released	296	358	*341*	*269*	*222*
Information part released	171	196	*211*	*231*	*206*
Information not held	97	81	*88*	*123*	*109*
Information withheld – cost of compliance	53	64	*63*	*36*	*27*
Exemptions applied	127	147	*159*	*171*	*139*
Vexatious request	0	0	*0*	*0*	*0*
Other (further clarification requested and not provided, invalid request, request withdrawn, redirected)	16	10	*13*	*4*	*9*

* 17 FOI requests still outstanding at time of report

Note: some responses fall into more than one category

10 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 2019/20, the Information Governance team published several Intranet Featured Adverts. Topics covered included inappropriate sending of information to home email addresses, permitted use of clinical systems, Phishing identification, etc.

10.1 eLearning

All NHS Borders staff members are required to be fully familiar with the concepts and principles of information governance. As well as providing ad hoc, face to face training and awareness sessions, an e-learning package is part of the suite of mandatory training for 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 relates directly to the Information Governance Code of Conduct. Staff members are required to complete this module every two years and a snapshot of figures taken on 1st April 2019 shows that 2905 out of a workforce of 3721 had undertaken this training. This represents 78% of all staff which is a sustained improvement but still requires management to actively encourage their staff to undertake this mandatory training.

An email to staff who had not completed the mandatory training was issued in February 2020 by Cliff Sharp, Medical Director and June Smyth, Senior Information Risk Owner. This was successful in encouraging fuller compliance and a similar exercise will be repeated throughout 2020.

11 Patient Information

NHS Inform is Scotland's national health information service. Their aim is to provide the people in Scotland with accurate and relevant information to help them make informed decisions about their own health and the health of the people they care for.

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.

These are also published on our intranet and internet sites together with links to the NHS Inform website. A recent addition is the "*How the NHS handles your personal health information*" leaflet, screen shot below. http://intranet/resource.asp?uid=33611

12 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:

- Published new Data Protection policy reflecting overhaul in data protection legislation
- Continued to encourage completion of organisational Information Asset Register and performed several departmental reviews.
- Updated Information Governance Code of Conduct published
- Updated E-mail policy published
- Quarterly reporting of activity and performance for monitoring and recommendations by the committee of:
    - Data Subject Access requests
    - Freedom of Information requests
    - Incident reports
    - E-learning modules completed
    - Confidentiality statements signed

13 Issues & challenges for 2020/21

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 Scottish Government's Information Assurance Strategy, the eHealth Cyber Resilience Plan, the requirements of the Network and Information Systems Regulations, and the ongoing implementation of the Records Management Plan will continue to provide a focus for developing these areas of the service.

In addition, the Covid-19 pandemic will undoubtedly introduce further challenges to the limited resource of the Information Governance team.

13.1 The Public Records (Scotland) Act 2011

The Public Records Scotland Act, 2011 (PRSA) specified standards of record management and accountability to the public sector with the aim of improving efficiency. NHS Borders Records Management Plan (2016) is published on the Internet and further work is required on the plan which will require input from the Information Governance team in the coming year.

The ongoing completion of the Information Asset Register will also address one of the requirements of the PRSA so it is essential this is maintained as part of each departments' Business as Usual tasks.

13.2 Cyber Essentials

Cyber Essentials certification is planned for July 2020 although the impact of Covid-19 may affect the timeline due to the availability of external assessors.

13.3 Raising awareness

During 2019/20 the Information Commissioner took enforcement action against several organisations and individual staff members in the UK for breaching data protection. Actions included prosecutions for unlawfully accessing health and social care records with no business need to do so. No action was taken against any Scottish Health organisation.

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. Further use of the "Featured Advert" facility and attendance at team meetings to remind staff of their Information Governance obligations are all planned for the coming year.

13.4 Incident reporting

It remains a key priority on the IG Action Plan to promote staff awareness of what constitutes an information governance incident, and that these are properly reported on Datix and followed up as appropriate.

13.5 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 this post will again be a priority in the coming year.

In addition to providing Data Protection services to NHS Borders, the Scottish Government has indicated that Health Boards must also offer the services of the Data Protection Officer (DPO) to all General Practices within the Health Board Area. Some funding has been made available by the SG so work is ongoing to introduce the DPO service to General Practice during 2020.

Statement of Approval

This report has been produced in line with the NHS Borders Annual Accounts for the year ended 31 March 2020. 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: Cliff Sharp, Medical Director, Chair of Information Governance Committee

Signed (Cliff Sharp) **Date**

Appendix 1: Information Governance Committee Membership

Cliff Sharp	Medical Director, Chair
Tim Patterson	Caldicott Guardian, vice chair
Nicky Berry	Director of Nursing & Midwifery
Jackie Stephen	Head of IM&T
George Ironside	Senior Health Information Manager
June Smith	Director of Workforce and Planning, Senior Information Risk Owner (SIRO)
John McLaren	Employee Director
Elaine Cockburn	Head of Quality and Clinical Governance
Vacant	Training & Professional Development
Kim Carter	Finance
Tony Trench	Patient & Public Involvement (up till June 2019)

Representation from General Manager/Service Manager – Acute, Mental Health and Primary Care

In attendance

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer
Carol Graham	Freedom of Information Officer
Tom Little	Project Change Manager
Jill Bolton	Committee Administrator

Appendix 2: Dates of Meetings and Attendees

04 June 2019

Dr Cliff Sharp	Medical Director (Chair)
Tim Patterson	Director of Public Health and Caldicott Guardian
Jackie Stephen	Head of IM&T
George Ironside	Senior Health Information Manager
Tony Trench	Public Representative

In attendance:

Ian Merritt	Information Governance Lead
Carol Graham	Freedom of Information
Tom Little	Project Change Manager
Murray Leys	Chief Officer, Social Work Transformation
Marion Phillips	Minutes

02 September 2019

Dr Cliff Sharp	Medical Director (Chair)
Tim Patterson	Caldicott Guardian
John McLaren	Employee Director
Kim Carter	Senior Finance Manager
George Ironside	Senior Health Information Manager
Justin Wilson	Clinical Information Co-ordinator (for Laura Jones)

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer
Tom Little	Project Change Manager
Jill Bolton	Minutes

02 December 2019

Dr Cliff Sharp	Medical Director (Chair)
George Ironside	Senior Health Information Manager
Karen Maitland	Assistant Service Manager - Unscheduled Care
Justin Wilson	Clinical Information Co-ordinator (for Laura Jones)

In attendance:

Ian Merritt	Information Governance Lead
Tom Little	Project Change Manager
Jill Bolton	Minutes

March 2019 **Cancelled due to Covid-19**