

Information Governance Committee Annual Report

2020/21

Contents

Introduction.....	3
1 Overview.....	4
1.1 Information Assurance Strategy	4
2 Structure	4
2.1 Information Governance Team	4
2.2 Information Governance Committee	4
2.3 Cyber Security Group	5
3 Policy & Planning.....	5
3.1 Information Governance Work Plan	5
3.2 Brexit	6
3.3 Information Governance Staff Code of Conduct	6
4 Caldicott Guardianship	6
5 Records Management.....	8
6 Subject Access Requests	9
7 Information Security.....	10
7.1 Standards and Guidance Documentation	10
7.2 Privacy Breach Detection Project	11
8 Incident Reporting.....	12
9 Freedom of Information	13
9.1 Activity	13
9.2 Response Times	13
9.3 Reviews & appeals	14
9.4 Performance monitoring	14
10 Training & Awareness.....	15
10.1 eLearning	15
11 Patient Information.....	15
12 Best Value	16
13 Issues & challenges for 2021/22.....	16
13.1 Raising awareness	17
13.2 Incident reporting	17
13.3 Resources	17
Statement of Approval	17
Appendix 1: Information Governance Committee Membership	18
Appendix 2: Dates of Meetings and Attendees	19

Introduction

This, the fourteenth NHS Borders Information Governance Annual Report, covers the financial year 2020/21 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 UK General Data Protection Regulation
- 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
- NHS Data Quality Assurance (Data Accreditation)
- Information Security Standard
- Caldicott Guardianship
- Network & Information Systems Regulations 2018

The Covid-19 pandemic has seen the NHS face unprecedented challenges over the past 12 months stretching resources to meet the demand on frontline services. Information Governance within NHS Borders was affected as technology was rolled out, and being involved in a number of agreements put in place nationally to support the response to the pandemic.

With the national lockdown, NHS Scotland accelerated the programme to roll out Microsoft Teams as the precursor to the full Office 365 package. IM&T rolled out equipment and services to accommodate a much greater number of staff to work from home, increasing the safety of staff and the delivery of services. The Information Governance team involvement in the introduction of Teams included publishing guidance documents on how to maintain a secure environment whilst working from home.

There were numerous national and local initiatives related to data sharing for projects involved with contact tracing, Covid testing and vaccination hubs. These all required input from the Information Governance team to ensure the principles of data protection were still adhered to.

As in previous years the team has continued to publish "Featured Adverts" on the Intranet providing hints and tips to all staff keeping them and NHS Borders secure. Current completion of the Information Governance online learning module, common with other online training, has fallen during the past year. A concerted effort will be made in 2021/22 to improve this position as staff having a sound understanding of the key aspects of information and cyber assurance is key to mitigating the risk to NHS Borders from loss of data or a cyber-attack.

It is expected that much of the 2021/22 will continue to be affected by the response to, and recovery from the Covid-19 pandemic, and safeguarding NHS Borders data will continue to feature in these plans.

Lynn McCallum
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
- Cyber 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 Strategy¹, in particular Domain B, and the Health and Social Care Information Sharing Strategy 2014-2020² 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. With the retirement of the Senior Health Information Manager in 2021 the opportunity is being taken to implement a new structure to improve the resources required to meet the additional demands from cyber assurance and records management under an Information Governance and Cyber Assurance Manager position.

2.2 Information Governance Committee

The Committee met, via Teams, on two of the planned four occasions in the year with the other two scheduled meetings 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

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/>

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

2.3 Cyber Security Group

The Cyber Security Group provides operational level guidance and monitoring on cyber security issues and to reports performance and compliance to the Information Governance Committee. The Head of IM&T, Senior Health Information Manager and the respective leads on information governance and cyber security 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 an organisation's basic security controls that will protect against a wide variety of the most common cyber-attacks and NHS Borders is committed to achieving this.

The Network and Information Systems Regulations (2018) (NIS) places a legislative obligation on Operators of Essential Services (OESs) of which NHS Scotland is one. The Scottish Health Competent Authority (SHCA) carried out a preliminary audit in Q4 2020. The results have been assessed and a project plan and action plan have been developed. These plans are being actively progressed. A further audit is scheduled for NHS Borders in September 2021.

3 Policy & Planning

3.1 Information Governance Work Plan

The March 2021 version of the Information Governance work plan breaks the workload of the IG Team into 6 work streams:

- Cyber Assurance
- General Practice
- Information Governance / GDPR
- IT Security
- Records Management
- Business as Usual

The plan will be used to schedule their work and provide exception reports to the Information Governance Committee at the quarterly meetings with a focus on work planned for the next 6 months. Capacity to meet immediate demands on the Team continued to be a challenge in 2020/21 but after September 2021 there should be additional capacity to progress the plan.

The IG team also worked on a range of areas during 2020/21. These include:

- Collaborating with the national Information Governance group to produce DPIAs and associated Agreements relating to Covid 19 data sharing initiatives
- Producing guidance material for staff relating to use of Teams and other Office 365 products
- Producing Data Processing Agreements and Data Protection Impact Assessments for several projects including:
 - Cytosponge
 - Drug and Alcohol Information System (DAISy)
 - Internet Enabled Cognitive Behavioural Therapy (IESO)
 - Non-Fatal Overdose
 - Contact tracing
 - Trojan – Patient monies system
 - Medtronic Carelink Pacemaker Monitoring

3.2 Brexit

On 31st January 2020, the UK withdrew from the European Union. European law, including the EU General Data Protection Regulation (EU GDPR) continued to apply until the end of the transition period on 31st December 2020. From that date, the UK General Data Protection Regulation (UK GDPR) as incorporated into the law of the United Kingdom under the European Union (Withdrawal) Act 2018, came into force.

The Trade and Co-operation Agreement between the UK Government and the EU, provides the ability to continue data transfers between the UK and the EU for up to 6 months (i.e. until the end of June 2021 or until the draft decision of adequacy is ratified).

On 19th February 2021, the European Union issued a draft decision of adequacy³ to the United Kingdom which, if approved, will enable the continuing free flow of personal information between the two administrations for a further 4 years (longer if renewed at that time). The decision is now firmly in the process of being ratified by the EU. The decision will pass through numerous committees, stakeholders and finally the European Parliament.

At March 2021 it is considered likely that the draft decision of adequacy will be approved by the European Union. This is because, among other details, the UK GDPR is based on retained EU legislation so the data protection rules in the United Kingdom in many aspects closely mirror the corresponding rules applicable within the European Union.

Should the draft decision not be approved for any reason, the UK will become a “third country” as far as data processing is concerned, meaning the member states in the EU will no longer be able to freely send personal data to the UK, without there being additional protection in place. This may mean new data protection clauses, known as Standard Contract Clauses or SCCs, in contracts with organisations based in the EU that we require to send personal information to us.

3.3 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 to this have been required over the past 12 months.

4 Caldicott Guardianship

Over the last year there were 8 applications for access to patient identifiable information which is a decrease of 64% on the previous year which is assumed to be due to the pandemic. Most requests were from NHS Borders staff requesting access to patient records for clinical systems such as BadgerNet and EMIS Community Web, with one to comply with Information Governance protocols.

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.

³ https://ec.europa.eu/info/sites/info/files/draft_decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_19_feb_2020.pdf

Table 4.1: Outcome of applications to the Caldicott Guardian, 2020/21

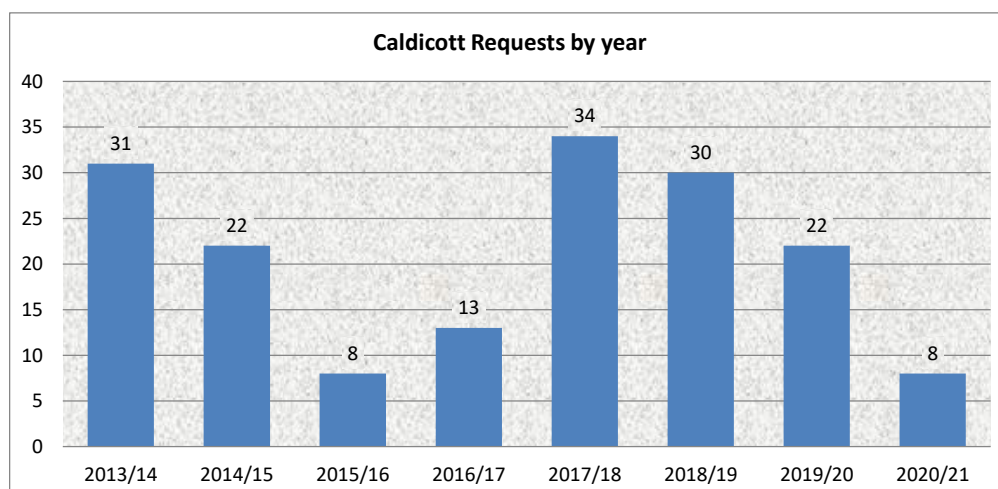
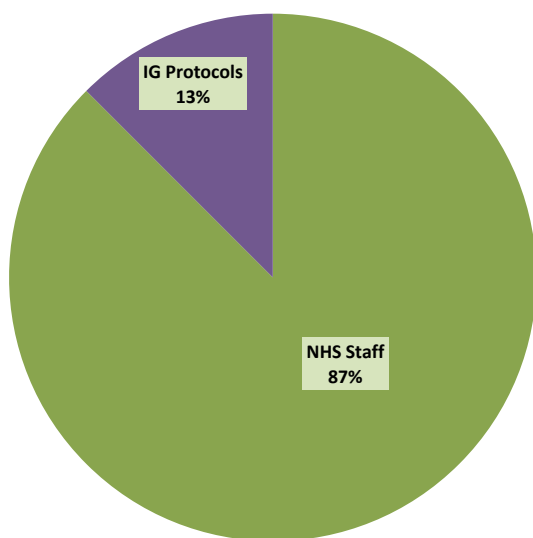


Table 4.2: Types of applications received by the Caldicott Guardian, 2020/21

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

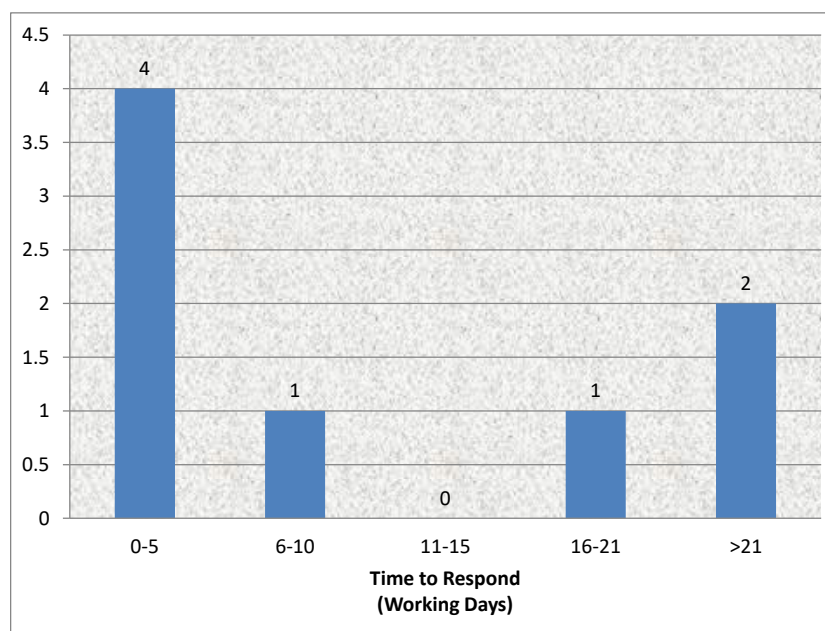
All applications were approved and no conditions were required to be applied or further safeguards to protect data security and confidentiality were necessary.

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



Application type	Number
Audit	
Research	
NHS Staff	7
IG Protocols	1
IM&T	
Access by Relative	
Other	
Total	8

Chart 4.3: Time to process Caldicott applications, 2020/21



5 Records Management

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 department's Business as Usual tasks.

In December 2020, a Progress Update Report (PUR) was submitted to the Keeper of the Records of Scotland detailing the work that is still required to be completed on the Records Management Plan. Specifically, the items that need to be addressed are:

Work item	Current status
Business Classification Scheme (Element 4)	Local schema expected to be replaced by a common national system.
Archiving (Element 7)	Discussions to be progressed with both Live Borders and University of Edinburgh
File Naming Convention and Version Control (Element 11)	Guidance document issued via Clinical Executive Operational Group in February 2021

In June 2020, the Scottish Government released the new Health and Social Care Code of Practice on Records Management. This replaced the 2012 version of the NHS Code of Practice for Records Management. The Information Governance team will continue to support managers and provide guidance on interpreting the retention periods for different record types as outlined in the Health and Social Care Code of Practice. The NHS Borders Records Management Policy has been updated to reflect the changes in the SG Code of Practice.

6 Subject Access Requests

Under Data Protection legislation (GDPR and Data Protection Act 2018), 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 number of requests received by the Subject Access team over the past 12 months has been significantly less than the previous year. Requests are up down by 33% on the previous 12 months. It is likely that the Covid-19 pandemic and the reduction in patient activity has played a part in this drop in requests.

Chart 6.1: Subject Access Requests by Year 2007/08 – 2020/21

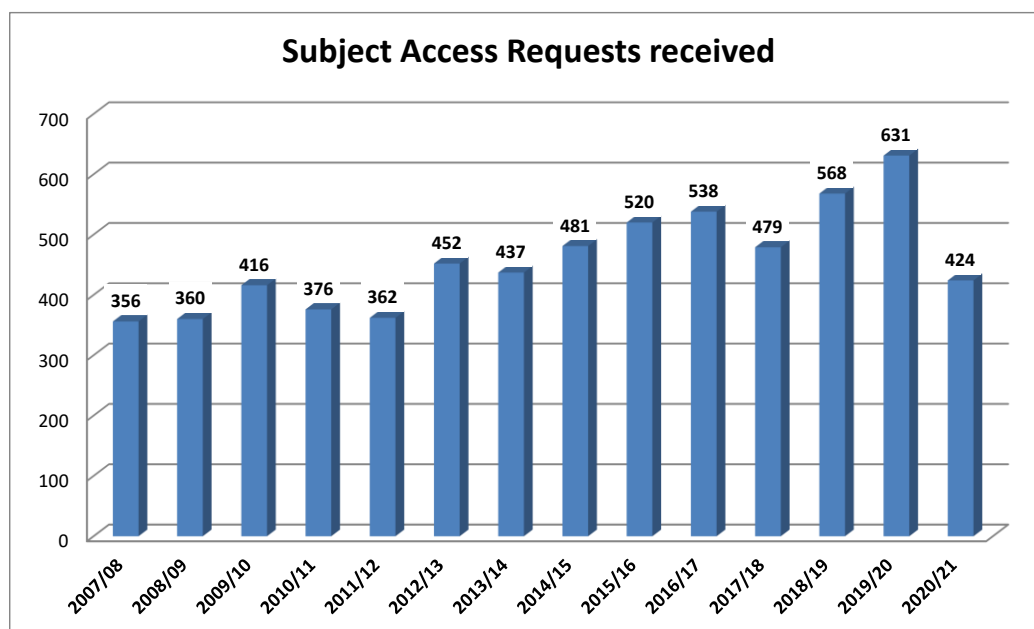


Chart 6.2: Subject Access Requests by Quarter 2020/21

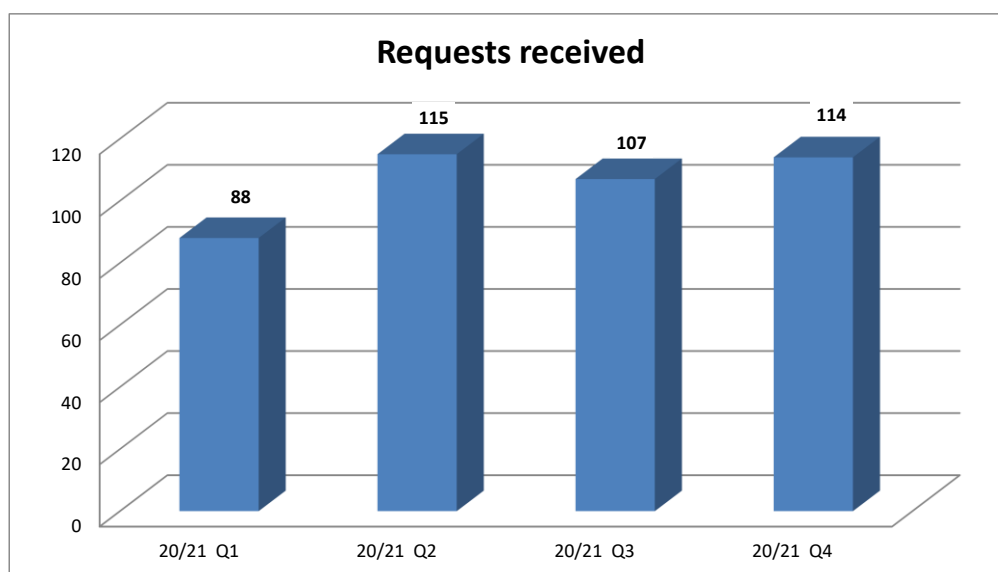
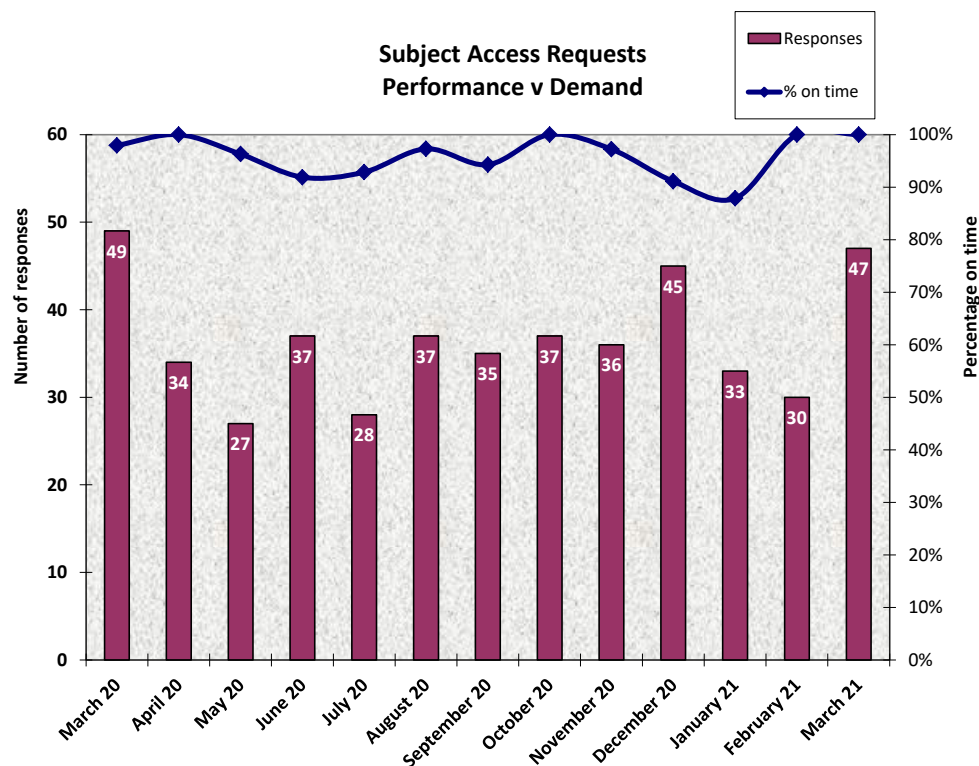


Chart 6.2: Subject Access Requests by Quarter 2020/21

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 96%, similar to 2019/20 (95%).

In total, 18 requests were responded to beyond the permitted one month period. The causes for the delay were:

Delay in receiving authorisation from clinician	50%
CD Burner failure (Radiology images)	11%
Notes returned late to Medical Records	11%
Medical Records staffing	28%

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. These are available on the Information Governance intranet page. During 2020/21 work continued to revise and update these documents in accordance with good practice guidelines.

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 on 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 14% during 2020/21 on the previous year. Of the 10,503 potential incidents, 87 cases were referred to line management for further investigation. This is down 46% on the previous year. As shown in the tables below, the number of confirmed incidents had a small decrease, of 12%, on the previous year to 30. The number of confirmed incidents over the past few years has remained consistent in the low 30s and this year is no exception. There was a noticeable spike of new staff members, typically in the vaccination hubs, viewing their own and family member records soon after commencing in post. This was addressed by reiterating the message given during initial training.

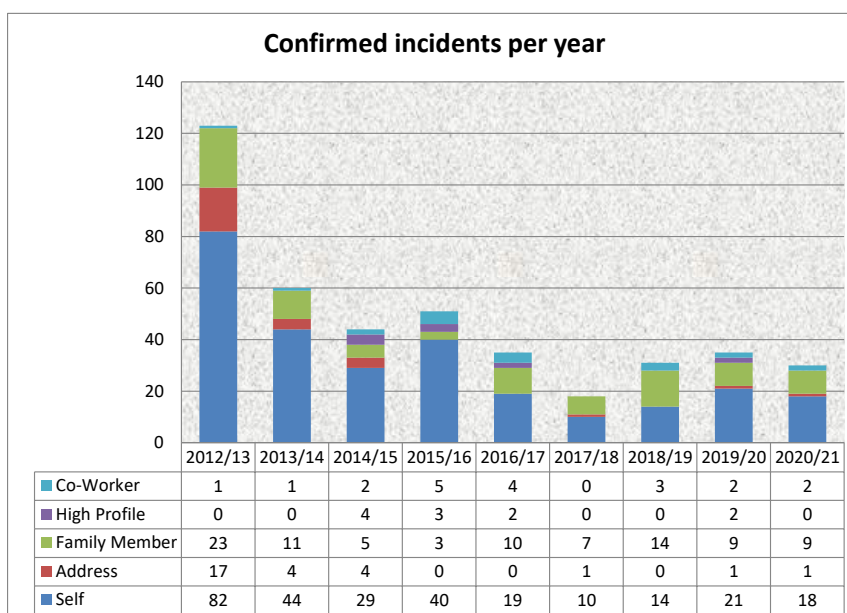
The breakdown of the confirmed incidents is shown in the chart and table below.

Chart 7.1: Privacy breach detection investigations and outcomes

The number of *potential* incidents (those where the predefined criteria were met) identified by FairWarning was down by 14% during 2020/21 on the previous year. Of the 10,503 potential incidents, 87 cases were referred to line management for further investigation. This is down 46% on the previous year. As shown in the tables below, the number of confirmed incidents had a small decrease, of 12%, on the previous year to 30. The number of confirmed incidents over the past few years has remained consistent in the low 30s and this year is no exception. There was a noticeable spike of new staff members, typically in the vaccination hubs, viewing their own and family member records soon after commencing in post. This was addressed by reiterating the message given during initial training.

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

Chart 7.1: Privacy breach detection investigations and outcomes



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.

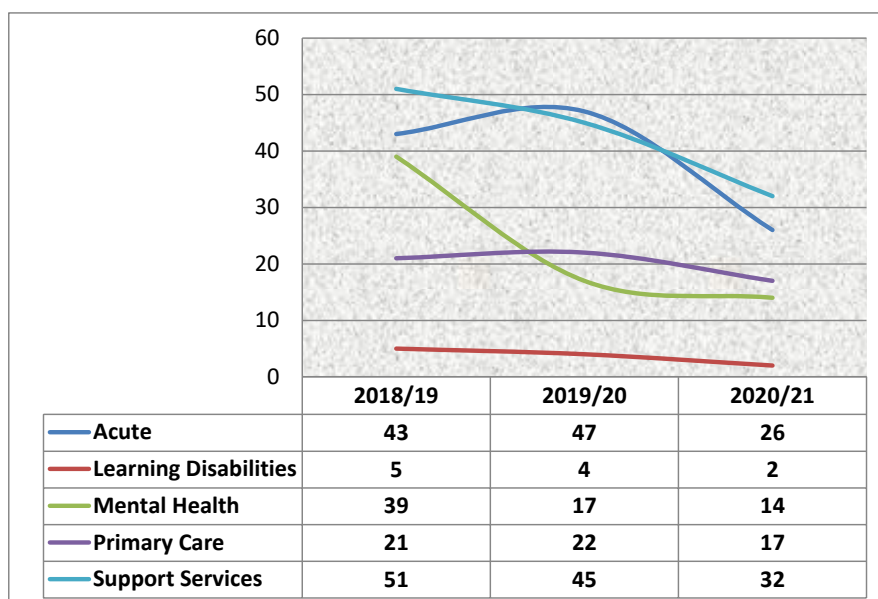
The tables below summarise the incidents reported over the past 12 months. There has been a 33% decrease in the number of incidents reported (91) compared with the previous year (135). Carelessness/human error continues to be the cause of the majority of incidents with confidential information being sent to or left in inappropriate locations. As noted in Section 7.2, Inappropriate Access to health records also remains at a consistent level.

A staff member was investigated for accessing health records without having a legitimate NHS purpose. The case was referred to the Information Commissioner's Office (ICO) who decided, after further investigation, that the actions taken by the Board had been sufficient.

Table 8.1: Summary of Types of Incident

Incident class	Incident Summary	2018/19	2019/20	2020/21
Breach of Confidentiality	Confidential information emailed to inappropriate destination	25	14	14
	Confidential information found in public/inappropriate place	15	13	8
	Confidential information sent to wrong recipient	25	23	24
	Confidential waste left insecure	2	1	1
	Information divulged carelessly	9	11	4
	Information divulged intentionally	4	1	1
	Permitted password to be used by other person	0	0	0
Breach of Confidentiality Total		80	63	52
Failing to Secure	Confidential information emailed without appropriate security	1	2	1
	Confidential information sent but not received	2	0	1
	Hardcopy confidential information sent using inappropriate method	0	1	2
	Hardcopy confidential/sensitive data lost/misplaced/stolen	20	14	1
Failing to Secure Total		23	17	5
Inappropriate Access	Accessed acquaintance/friend record (FW)	1	0	1
	Accessed clinical records without due reason (Not FW)	4	2	1
	Accessed family member record (FW)	5	8	6
	Accessed neighbour record (FW)	0	0	0
	Accessed other person's record inappropriately (FW)	0	1	1
	Accessed own record (FW)	11	14	16
	Accessed work colleague record (FW)	3	2	0
	Used password of other person	0	1	0
Inappropriate Access Total		24	28	25
Incorrectly filed	Patient documents/labels found in wrong record	29	27	8
	Patient documents/labels not filed at all or not in correct place in record	3	0	1
Incorrectly filed Total		32	27	9
Grand Total		159	135	91

Table 8.2: Summary of Incidents by reporting Clinical Board



9 Freedom of Information

The Freedom of Information (Scotland) Act 2002 (FOISA) introduced in January 2005 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 an increase in the number of requests but in this unprecedented year we have seen a decrease in requests due to 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 2020/21 seeing a decrease of 11% on the previous year. Requests from the Commercial sector now account for the highest volume of work at 33% with those from the Media at 20%. Requests from Scottish Parliament have risen to 18% of the total number of requests received but this was mainly due to Coronavirus Covid 19 Pandemic. The other categories have all slightly decreased, again due to the Coronavirus Covid 19 pandemic.

9.2 Response Times

The Act requires that all requests are responded to within 20 working days. During the year 2020/21 our compliance increased to an average of 96%.

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, we published updates on our public website informing applicants of the reasoning behind the delays. This was to try and help reduce the likelihood of the applicant complaining to the Scottish Information Commissioner (OSIC).

NHS Borders received guidance at the start of April 2020 from OSIC stating that they were temporarily extending the 20 working day deadline to 60 working days until 30 September 2020. Unfortunately half way through this period they rescinded this extension and therefore all requests had to be responded to within the 20 working days. This caused issues with our response deadlines and therefore the report shows that we breached the regulations on 16 occasions.

Table 9.1: Compliance with statutory deadline

	2020/21	2019/20	2018/19	2017/18	2016/17
Total number of requests responded to	502	566	622	617	623
Number of requests answered within 20 working days	482	533	616	594	619
Number of requests answered in more than 20 working days	16	16	6	23	4
Median number of days taken to respond	12	10	11	12	14
Percentage compliance	96%	94%	99%	96%	99%

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 2020/21 we received no 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.

Table 9.2: Outcome of requests

	2020/21	2019/20	2018/19	2017/18	2016/17
All information released	259	296	358	341	269
Information part released	169	171	196	211	231
Information not held	49	97	81	88	123
Information withheld – cost of compliance	39	53	64	63	36
Exemptions applied	144	127	147	159	171
Vexatious request	0	0	0	0	0
Other (further clarification requested and not provided, invalid request, request withdrawn, redirected)	17	16	10	13	4

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 2020/21, the Information Governance team published several Intranet Featured Adverts. Topics covered included appropriate use of Microsoft Teams and data protection measures when working from home.

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 and virtual 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 25th February 2021 shows that 2419 out of a workforce of 3675 had undertaken this training. This represents 66% of all staff which is a drop on the previous year (78%).

It is considered likely that the disruption to services caused by the Covid-19 pandemic is the main reason for the drop in completion of the Information Governance online training. Plans are being made to address this under a wider piece of work on statutory and mandatory training in 2021/22.

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:

- 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 module completed (Confidentiality statements signed)

13 Issues & challenges for 2021/22

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 Strategic Framework for a Cyber Resilient Scotland⁴, 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.

⁴ <https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2021/02/strategic-framework-cyber-resilient-scotland/documents/strategic-framework-cyber-resilient-scotland/strategic-framework-cyber-resilient-scotland/govscot%3Adocument/strategic-framework-cyber-resilient-scotland.pdf>

13.1 Raising awareness

During 2020/21 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.

13.2 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.

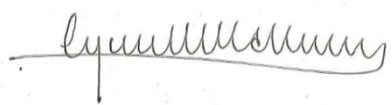
13.3 Resources

Following the Scottish Government advising that Health Boards are to offer a Data Protection Officer Service to General Practice, a new Data Protection Facilitator post within the Information Governance team has been filled by Julie Dickson, who had been the Information Governance Officer. Interim arrangements have been put in place to cover the BAU tasks of the Information Governance post. Following the retirement of the Senior Health Information Manager the opportunity has been taken to strengthen the team with this post to be replaced by an Information Governance & Cyber Assurance Manager, along with plans for a Records Manager and Cyber Assurance Lead positions.

Statement of Approval

This report has been produced in line with the NHS Borders Annual Accounts for the year ended 31 March 2021. 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: Lynn McCallum, Medical Director, Chair of Information Governance Committee



Signed

(Lynn McCallum)

Date 21 April 2021

Appendix 1: Information Governance Committee Membership

Lynn McCallum	Medical Director, Chair
Tim Patterson	Caldicott Guardian, vice chair
June Smyth	Director of Workforce and Planning, Senior Information Risk Owner (SIRO)
Nicky Berry	Director of Nursing & Midwifery
Catherine Kelly	Chief Clinical Information Officer
Jackie Stephen	Head of IM&T
George Ironside	Senior Health Information Manager
John McLaren	Employee Director
Kim Carter	Finance
Laura Jones	Head of Quality and Clinical Governance
Vacant	Training & Professional Development
Representation from General Manager/Service Manager – Acute, Mental Health and Primary Care	

In attendance

Ian Merritt	Information Governance Lead
Julie Dickson	Data Protection Facilitator
Carol Graham/Alicia Jones	Freedom of Information Officer
Tom Little	Project Change Manager
Jill Bolton	Committee Administrator

Appendix 2: Dates of Meetings and Attendees

July 2020

Cancelled due to Covid-19

21 September 2020

Dr Lynn McCallum	Medical Director (Chair)
John McLaren	Employee Director
June Smyth	Director of Strategic Change & Performance and SIRO
George Ironside	Senior Health Information Manager
Justin Wilson	Clinical Information Co-ordinator (for Laura Jones)
Susan Henderson	Planning & Development Officer LDS
Pauline Burns	Clinical Service Manager

In attendance:

Ian Merritt	Information Governance Lead
Tom Little	Project Change Manager
Carol Graham	Freedom of Information Coordinator
Marion Phillips	Minutes

December 2020

Cancelled due to Covid-19 – Papers disseminated via email January 2021

23rd March 2021

June Smyth	Director of Strategic Change & Performance and SIRO (Chair)
John McLaren	Employee Director
Tim Patterson	Caldicott Guardian
Jackie Stephen	Head of IM&T
Catherine Kelly	Chief Clinical Information Officer
George Ironside	Senior Health Information Manager
Justin Wilson	Clinical Information Co-ordinator (for Laura Jones)
Kim Carter	Finance
Chris Myers	Service Manager, Primary Care
Sam Whiting	Deputy Hospital Manager

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Data Protection Facilitator
Kevin Messer	IT Service Delivery Manager
Alicia Jones	Freedom of Information Coordinator
Jill Bolton	Minutes