Information Governance Committee Annual Report

2018/19

Contents

Introduction

This is the twelfth NHS Borders Information Governance Annual Report and covers the financial year 2018/19 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 2018
- 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 have been dominated by the introduction of the European General Data Protection Regulation (GDPR) in May 2018. This represented the first major overhaul of data protection legislation in the UK for twenty years so it was naturally going to result in a large amount of work for the Information Governance team. The team have worked to establish a new procedure around the implementation of Data Protection Impact Assessments (DPIAs) for new initiatives that involve the processing of personal data. They have also produced a template to be used by departments as necessary to produce their own specific privacy notice. These will supplement the corporate privacy notice that is now published on the NHS Borders public website (http://www.nhsborders.scot.nhs.uk/privacy-notice/).

The changes introduced by the GDPR will continue to impact heavily on the Information Governance team's workload over the coming 12 months, including setting up Data Protection Officer services to General Practices throughout the Borders area.

EMIS Health has now replaced ePEX as the Community Patient Administration System. The new system is fully integrated into the FairWarning monitoring system meaning the Information Governance team now receive these additional reports daily. It is encouraging to report that, to date, no inappropriate use of patient information held in EMIS has been identified.

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 again be taken up consolidating improvements in information handling that come with the implementation of the 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, with the business of the 4th being carried out virtually. 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

[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/

In January 2019 it was agreed that work on Cyber Security should also be regularly reported to the Committee. 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 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 was reviewed and updated in March 2018. No further updates have been required over the last 12 months. Compliance with the policy in terms of learning and signing confidentiality statements continues to be monitored through performance scorecards.

The Information Governance Strategy still requires to be reviewed to take account of the NHS Scotland Information Assurance Strategy and the new data protection legislation. It is intended to explore whether a common strategy with NHS Lothian and NHS Fife might be developed, in line with the regional model direction of travel.

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 provide exception reports to the Information Governance Committee.

Basing the completion over a 12 month period and the tasks already assigned to the team, this established that there was approximately a 6 months gap between the estimated time required, and the time available within the team. Work is ongoing to review the priority of the tasks to firm up the assessment of the resource to deliver a revised plan.

Preparation and introduction of the General Data Protection Regulation required updating of procedures and introducing a number of additional processes. All sections of NHS Borders were approached to help establish a comprehensive NHS Borders Information Asset Register – this being a key foundation of information governance. Whilst the Register is in place, work, as highlighted in an Internal Audit report, remains to be progressed. Action has been taken to improve the Information Asset Register completeness over the first 6 months of 2019/20.

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

- **Updating the Information Governance eLearning Module** – This now includes elements relevant to GDPR and a separate section on Freedom of Information
- **Cyber Maturity Review and subsequent Public Sector Cyber Security Action Plan** – Contributing to these as a members of the cyber security team.
- **Producing Data Processing Agreements and Data Protection Impact Assessments** – have been produced for several projects including:
    - Radiology overnight reporting project
    - Intermittent Self Catheterisation Project
    - Migrating the Occupational Health system, Cohort, to a hosted service
- **Publishing test Phishing emails** – Used a product to test NHS Borders' exposure and vulnerability to Phishing emails (malicious emails designed to con the recipient into click untrusted links, ultimately resulting in a compromise of system security).

3.4 Information Governance Staff Code of Conduct

The NHS Borders Information Governance Code of Conduct for Staff, first published in 2011, has been further updated, to reflect the implementation of the GDPR. The Code of Conduct continues to be a mainstay of staff education and awareness on information governance matters. The updated version was approved by the Information Governance Committee in March 2019.

4 Caldicott Guardianship

Over the last year there were 30 applications for access to patient identifiable information which is a decrease of 12% on the previous year. Most requests (93%) 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, 2018/19

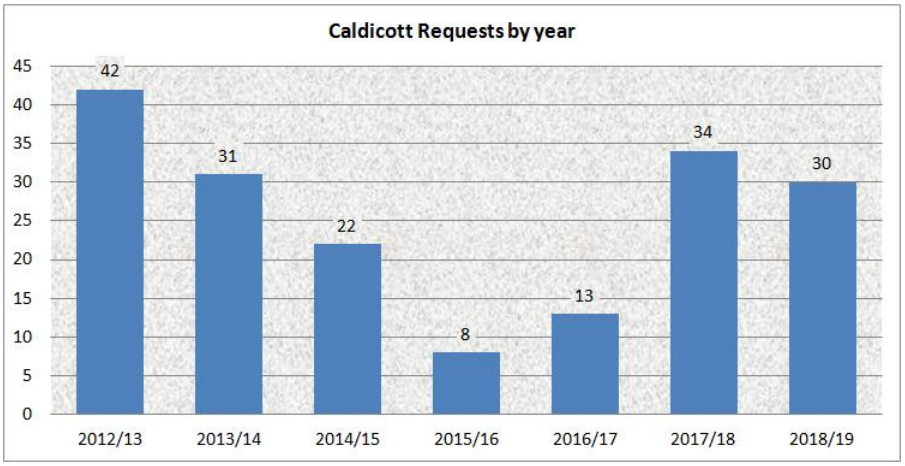
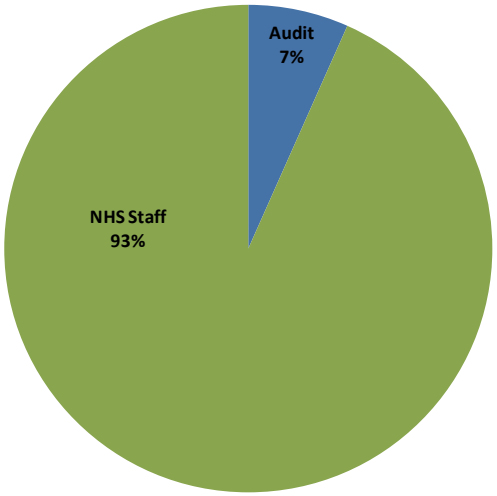


Table 4.2: Types of applications received by the Caldicott Guardian, 2018/19

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

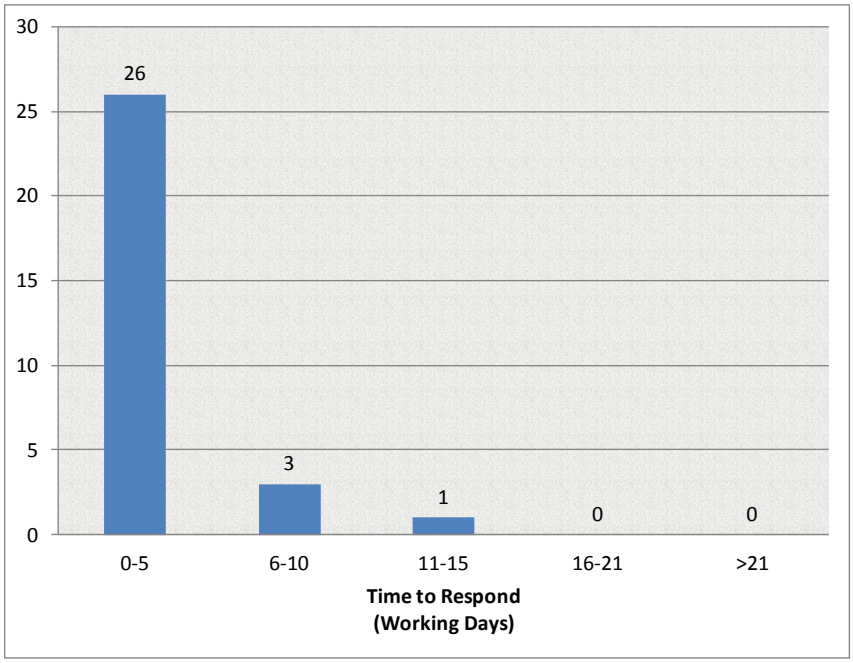


Application type	Number
Audit	2
Research	
NHS Staff	28
Information Governance	
IM&T	
Relative Access	
Other	
Total	**30**

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 all applications meeting the target.

Chart 4.1: Time to process Caldicott applications, 2018/19



5 Records Management

Public Records (Scotland) Act 2011

Progress on the 2016 Records Management Plan (RMP) has been limited. This is mainly because the Information Governance team concentrated on the implementation of the General Data Protection Regulation and the additional overhead associated with that.

Having an Information Asset Register as part of the requirements of the GDPR also effectively fulfils one of the requirements – having a Business Classification Scheme for the PR(S)A.

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 is expected in 2019.

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 has increased, in line with predictions, following the introduction of the General Data Protection Regulation in May 2018.

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 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 – 2018/19

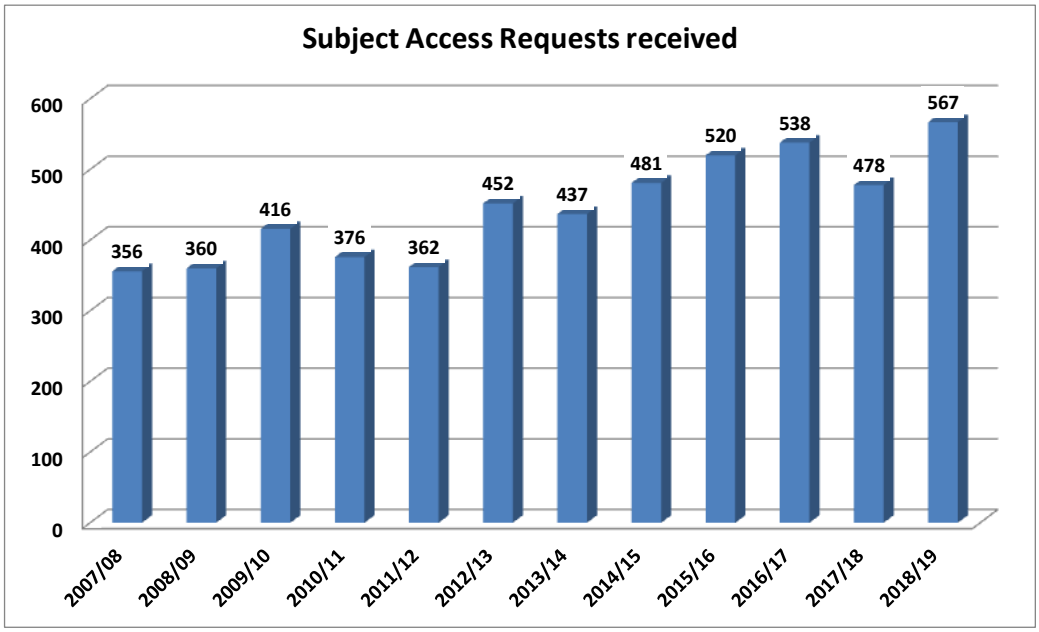


Chart 6.2: Subject Access Requests by Quarter 2018/19

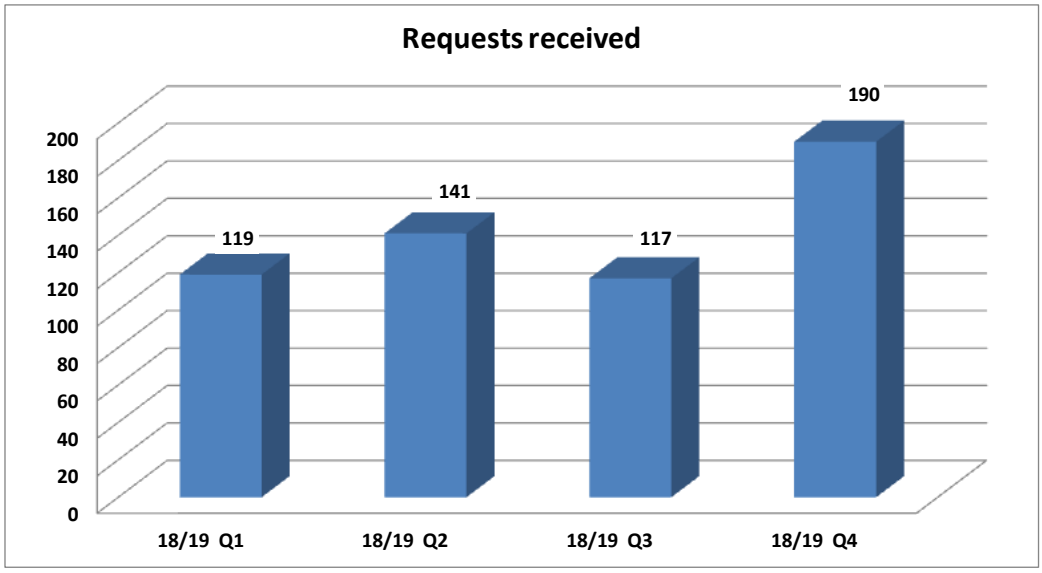
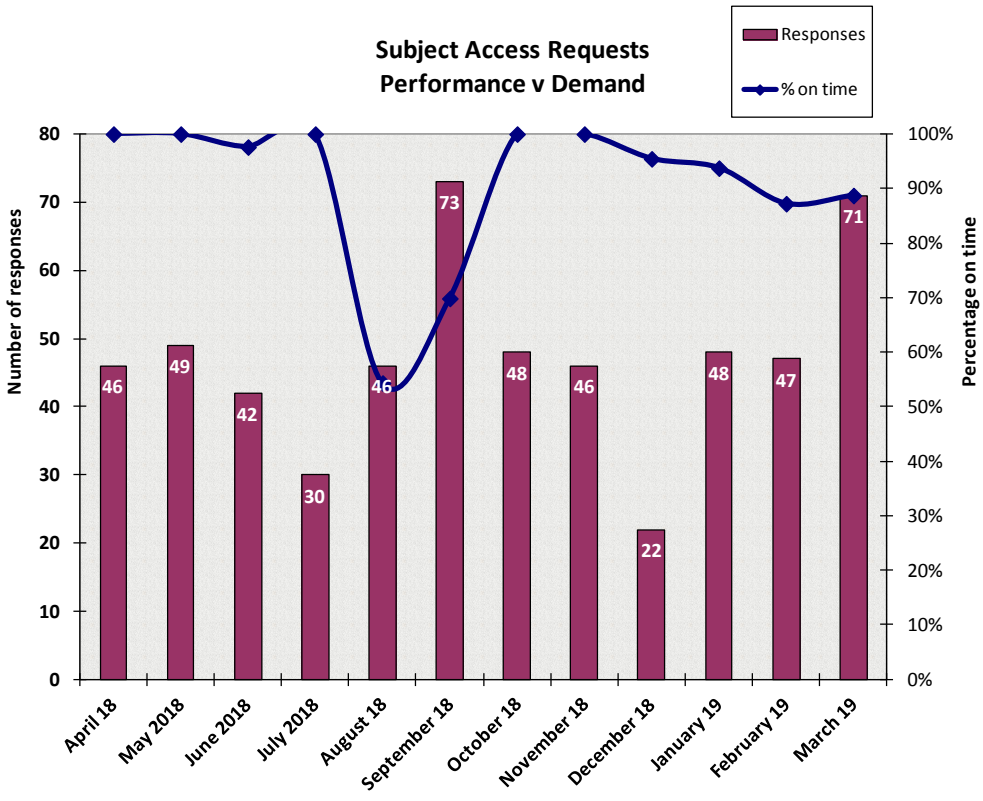


Chart 6.2: Subject Access Requests by Quarter 2018/19

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 compliance for the year was 91%. Although some of the 6% drop in performance must be attributed to increased numbers of requests the largest drop, in August and September, was due to the failure of CD burning facilities in Radiology, meaning requests for images could not be fulfilled.

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.

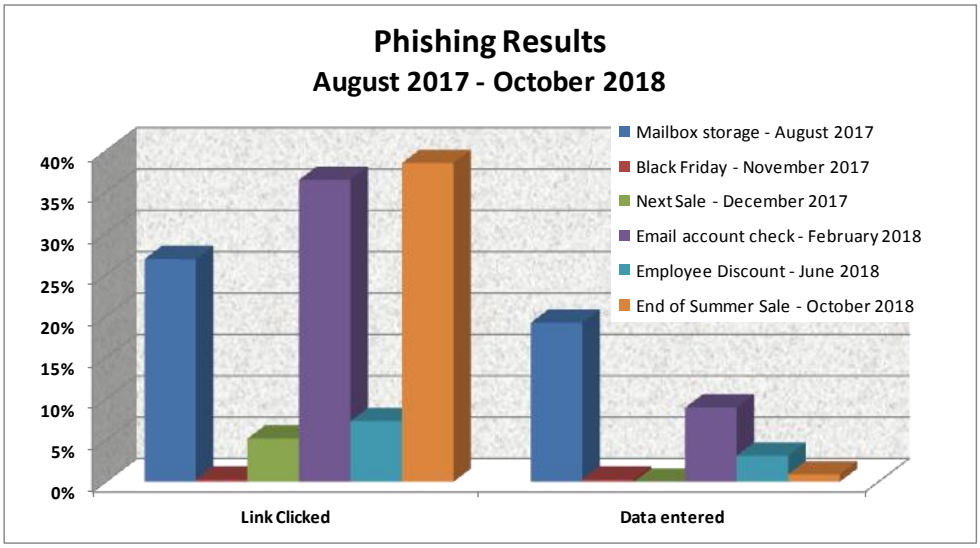
Following the 'Wannacry' cyber attack in May 2017, where NHS Borders in common with many other Boards and public sector organisations suffered significant disruption, the Scottish Government Resilience Unit published the *Cyber – Public Sector Action Plan* in November 2017. This placed obligations on all public sector organisations. In particular it required that they achieve *Cyber Essentials* (CE) certification as a minimum standard. NHS Borders Board have committed to achieving the higher standard of *Cyber Essentials Plus* (CE+) certification.

One of the requirements was to integrate cyber security more closely with Information Governance. The Information Governance Lead is now a member of the newly formed Cyber Governance Group. The Cyber Governance Group will be providing regular reports to the Information Governance Committee.

Phishing and Email Impersonation Attacks are a real risk to all organisations. Between late 2017 and October 2018 NHS Borders Information Governance issued several test Phishing emails to the organisation to test responses. Some were sent to random departments and others were sent to the whole organisation. The emails were all designed to replicate actual Phishing emails that have been discovered in circulation.

The purpose of the exercise was to see how readily people would click on unsolicited links or attachments and thus identify the level of risk to the organisation. When links in these specially crafted messages were clicked the email recipient was taken to an education and awareness page. The page explained about the dangers of clicking on links in emails and gave tips on how to identify a Phishing email. In addition the staff members' names and email addresses were recorded in a report so the Information Governance team could identify particular trends.

These confirmed how easy users can be tricked into clicking on malicious links in unsolicited emails. Further user education is planned during 2019/20.



Work has continued to formalise other 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 2018/19 work continued to revise and update theses 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 produced. This was necessitated following the implementation of the General Data Protection Regulation in May 2018.

7.2 Mobile Computing

Information Governance team has developed a Mobile Device policy to complement the existing technical security policies, in line with national guidelines. This is a fast developing area and it is expected that further work will be required in 2019/20.

7.3 European General Data Protection Regulation (GDPR)

The European General Data Protection Regulation (GDPR) is a significant update to the Data Protection Act 1998 requiring all organisations that process personal data of EU residents to comply with it. The biggest changes to current legislation are

- Consent must be explicit and provable (opt-in, not opt-out)
- Data breaches must be reported to a "Supervisory Authority" (the ICO) within 72 hours
- Fines for non-compliance up to £17 million
- Shortening of time limit to respond to Subject Access Requests to one month (from 40 days)
- Information in relation to a Subject Access Request must be provided free of charge
- Must be able to provide information in a commonly used electronic format
- Increased transparency of data processing – must publish data privacy notices
- Accountability – Compliance must be demonstrated not just implied

The mandatory annual fee for registration with the Information Commissioner's Office (ICO) increased from £500 to £2,900.

The GDPR introduces a mandatory requirement for all new initiatives (projects, procedures, policies, etc.) that involve the processing of personal information. If the processing will, or may, result in a high risk to the rights and freedoms of an individual then a Data Protection Impact Assessment (DPIA) must be completed prior to any processing commencing. A DPIA template was produced by the national Information Governance group and adopted in NHS Borders. The Information Governance lead has also produced a protocol document, intended to assist project managers in completing the DPIA. The Information Governance team have been involved in completing several DPIAs over the past 12 months and this is likely to increase as new corporate initiatives and requirements are introduced.

7.4 Privacy Breach Detection Project

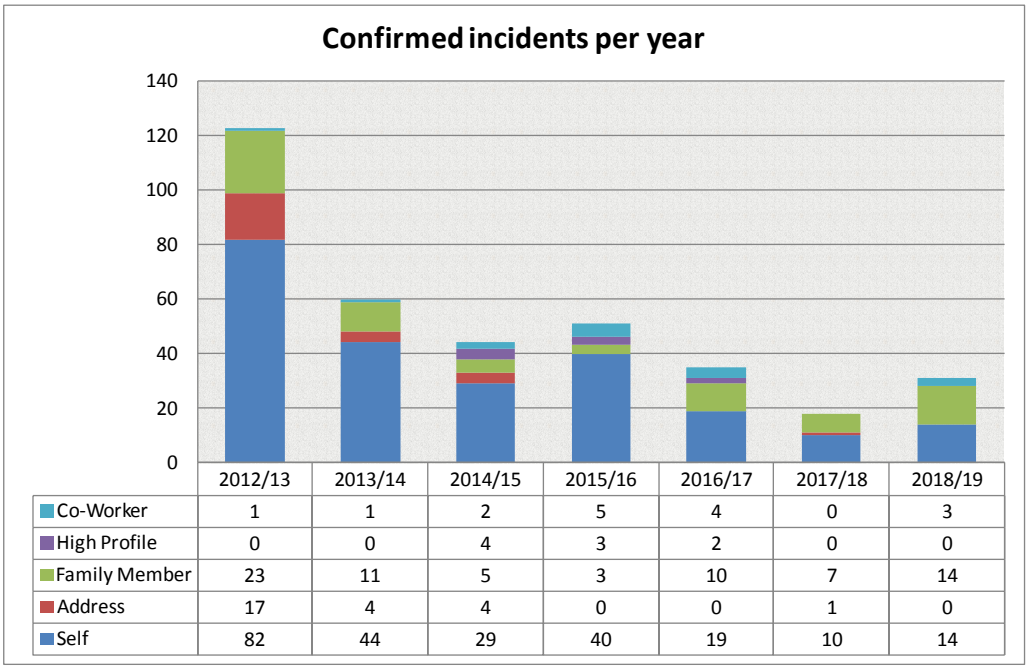
FairWarning remains the privacy breach detection tool used within NHS Borders and has been in operation since 2012.

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 16% during 2018/19 on the previous year. Of the 10,352 potential incidents 136 cases were referred to line management for further investigation. This is up 38% on the previous year. As shown in the tables below, the number of confirmed incidents also increased, by 44%, on the previous year to 32. 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 8.1: Privacy breach detection investigations and outcomes



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

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.

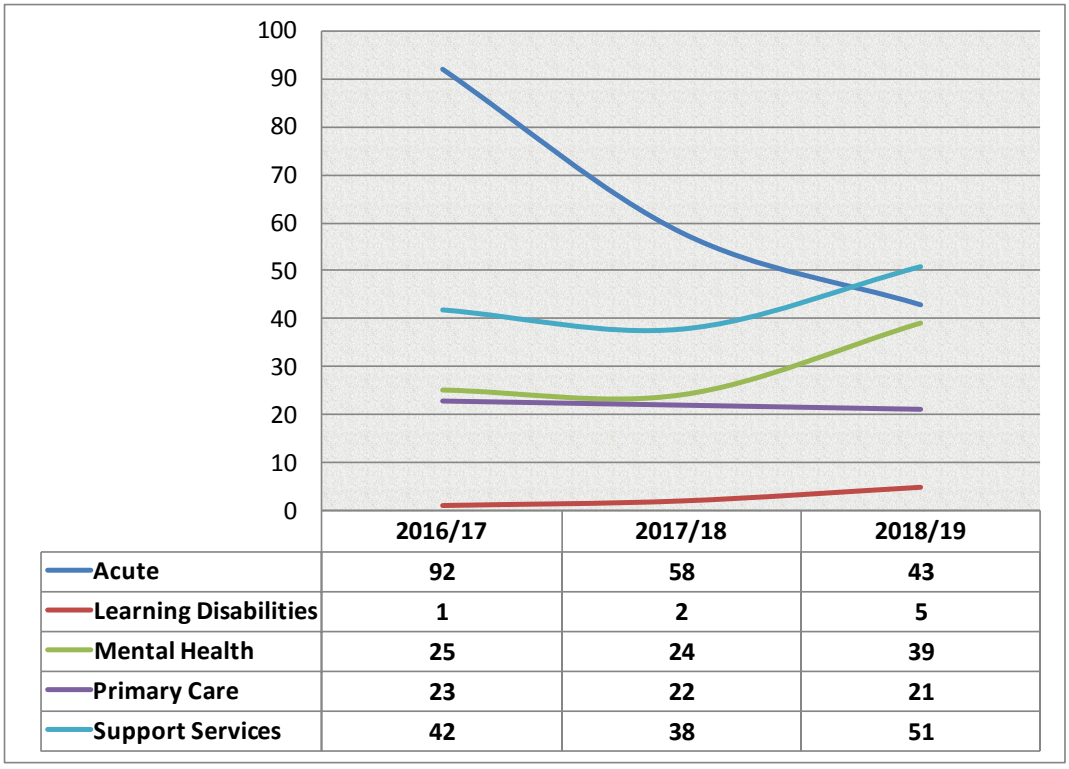
The tables below summarises the incidents reported over the past 12 months. There has been an increase in the number of incidents reported (159) compared with the previous year (144). However, this figure is very similar to the average over the past several years. Carelessness/human error appears to be the root cause of incidents where the numbers have risen. Information emailed to an inappropriate destination (typically a staff member's home address) and information divulged carelessly have both recorded increased instances.

The Acute area has continued the trend from the previous period of reducing the number of recorded incidents. Mental Health and Support Services have both seen increases in the numbers of incidents reported.

Table 9.1: Summary of Types of Incident

Incident class	Incident Summary	2016/17	2017/18	**2018/19**
Breach of Confidentiality	Confidential information emailed to inappropriate destination	6	19	25
	Confidential information found in public/inappropriate place	19	32	15
	Confidential information sent to wrong recipient	28	22	25
	Confidential waste left insecure	2	8	2
	Information divulged carelessly	13	0	9
	Information divulged intentionally	0	0	4
	Permitted password to be used by other person	1	0	0
Breach of Confidentiality Total		**69**	**81**	**80**
Failing to Secure	Confidential information emailed without appropriate security	2	1	1
	Confidential information sent but not received	2	1	2
	Hardcopy confidential information sent using inappropriate method	0	2	0
	Hardcopy confidential/sensitive data lost/misplaced/stolen	25	18	20
Failing to Secure Total		**29**	**22**	**23**
Inappropriate Access	Accessed acquaintance/friend record (FW)	0	1	1
	Accessed clinical records without due reason (Not FW)	1	0	4
	Accessed family member record (FW)	6	5	5
	Accessed neighbour record (FW)	0	0	0
	Accessed other person's record inappropriately (FW)	4	0	0
	Accessed own record (FW)	17	10	11
	Accessed work colleague record (FW)	3	0	3
	Used password of other person	3	0	0
Inappropriate Access Total		**34**	**16**	**24**
Incorrectly filed	Patient documents/labels found in wrong record	39	22	29
	Patient documents/labels not filed at all or not in correct place in record	12	3	3
Incorrectly filed Total		**51**	**25**	**32**
Grand Total		**183**	**144**	**159**

Table 9.2: Summary of Incidents by reporting Clinical Board



	2016/17	2017/18	2018/19
Acute	92	58	43
Learning Disabilities	1	2	5
Mental Health	25	24	39
Primary Care	23	22	21
Support Services	42	38	51

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 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. 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.

9.1 Activity

The volume of FOI requests increased with 2018/19 seeing an increase of 5.5% on the previous year. Requests from the media continue to account for the highest volume of work at 27% with those from the Commercial sector at 25%. The Scottish Parliament stayed the same and accounted for 22% of the total number of request received. 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 2018/19 our compliance increased to an average of 99%.

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 this helps to reduce the likelihood of the applicant complaining to the Scottish Information Commissioner.

Table 10.1: Compliance with statutory deadline

	2018/19	*2017/18*	*2016/17*	*2014/15*	*2013/14*	*2012/13*	*2011/12*
Total number of requests responded to	**622**	617	623	527	331	399	326
Number of requests answered within 20 working days	**616**	594	619	524	243	325	292
Number of requests answered in more than 20 working days	**6**	23	4	3	88	74	34
Median number of days taken to respond	**11**	12	14	12	20	19	18
Percentage compliance	**99%**	96%	99%	99%	73%	81%	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.

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 2018/19 we did not receive any 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 10.2: Outcome of requests

	2018/19	*2017/18*	*2016/17*	*2015/16*	*2014/15*	*2013/14*	*2012/13*
All information released	358	*341*	*269*	*222*	*202*	200	190
Information part released	196	*211*	*231*	*206*	*152*	84	137
Information not held	81	*88*	*123*	*109*	*83*	67	122
Information withheld – cost of compliance	64	*63*	*36*	*27*	*31*	41	83
Exemptions applied	147	*159*	*171*	*139*	*90*	22	46
Vexatious request	0	*0*	*0*	*0*	*0*	0	0
Other (further clarification requested and not provided, invalid request, request withdrawn, redirected)	10	*13*	*4*	*9*	*7*	9	10

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 2018/19, 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 2888 out of a workforce of 3812 had undertaken this training. This represents 76% of all staff, and although significantly up on the previous year (56%), still requires management to actively encourage their staff to undertake this mandatory training.

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:

- Produced and published an Information Asset Register designed to capture all of NHS Borders' information assets.
- Published several controlled Phishing emails using a tool to test the organisations ability to recognise and appropriately deal with this type of malicious email. Produced a report analysing the results.
- Revised E-mail policy approved
- Revised Information Governance Code of Conduct was approved
- Revised Data Protection policy was issued for consultation. Due to be published during Q1 2019/20

- Revised Information Governance Code of Conduct was approved
- 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 2019/20

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, 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 recent implementation of the European General Data Protection Regulation (GDPR) has introduced changes in practice, such as the introduction of Data Protection Impact Assessments (DPIAs), which further challenges 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 The European General Data Protection Regulation (GDPR)

The GDPR came into force on 25th May 2018, along with the UK Data Protection Act 2018. The changes to this legislation represent the biggest changes in Data Protection law in twenty years. Work is ongoing to ensure that NHS Borders remains compliant with the new law.

One element of the new law is Accountability – it is not enough just to be compliant: compliance must be demonstrable. This requires:

- The implementation, and ongoing maintenance, of an Information Asset Register
- Introducing "Privacy by Design" to all projects involving personal identifiable information
- Performing a Data Protection Impact Assessment on new processes that involve personal identifiable information before the processing commences
- Documenting how personal identifiable information is processed in published Privacy Notices
- Reporting personal data breaches to the ICO

The Information Governance team will continue to develop and implement procedures and processes to support the above requirements and it is anticipated that this will account for a significant amount of the team's resources over the coming year.

13.3 Public Sector Cyber Resilience Action Plan

In November 2017, Scottish Cabinet Secretary, wrote to all Scottish Health Boards with a requirement to ensure each organisation implements the Scottish Public Sector Action Plan on Cyber Resilience. The plan has specific targets for completion of the 11 Key Actions, including undertaking an independent Cyber Essentials assessment and implementing the resultant findings. Information Governance will again be members of the team working on this in the forthcoming year.

13.4 Raising awareness

During 2018/19 the Information Commissioner took enforcement action against several organisations in the UK for breaching data protection. 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.

13.5 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.

13.6 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.

Statement of Approval

This report has been produced in line with the NHS Borders Annual Accounts for the year ended 31 March 2019. 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

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
Jill Bolton	Committee Administrator

Appendix 2: Dates of Meetings and Attendees

26 June 2018

Dr Cliff Sharp	Medical Director (Chair)
Tim Patterson	Caldicott Guardian
Kim Carter	Senior Finance Manager
Anne Palmer	Clinical Governance and Quality (for Ros Gray)
George Ironside	Senior Health Information Manager
Tony Trench	Public Representative

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer (minutes)
Carol Graham	Freedom of Information

25 October 2018 (postponed from September)

Tim Patterson	Caldicott Guardian
Kim Carter	Senior Finance Manager
Anne Palmer	Clinical Governance and Quality (for Ros Gray)
George Ironside	Senior Health Information Manager
Tony Trench	Public Representative
Jackie Stephen	Head of IM&T
Dr Cliff Sharp	Medical Director (Chair)

In attendance:

Ian Merritt	Information Governance Lead
Julie Dickson	Information Governance Officer

December 2018 **Cancelled (Virtual meeting paper work issued 31 January 2019)**

05 March 2019

Dr Cliff Sharp	Medical Director (Chair)
George Ironside	Senior Health Information Manager
Karen Maitland	Assistant Service Manager - Unscheduled Care
Pauline Burns	Clinical Service Manager
Jackie Stephen	Head of IM&T
Kath Liddington	Professional Training and Development

In attendance:

Ian Merritt	Information Governance Lead
Carol Graham	Freedom of Information
Tom Little	Project Change Manager
Jill Bolton	Minutes