



# **Information Governance Committee Annual Report**

**2017/18**

## Contents

<b>Introduction .....</b>	<b>3</b>
<b>1 Overview .....</b>	<b>5</b>
1.1 Information Assurance Strategy .....	5
<b>2 Structure .....</b>	<b>5</b>
2.1 Information Governance Team .....	5
2.2 Information Governance Committee .....	5
<b>3 Policy &amp; Planning .....</b>	<b>5</b>
3.1 Records Management Policy .....	5
3.2 Information Governance Policy .....	6
3.3 Information Governance Action Plan .....	6
3.4 Information Governance Code of Conduct for Staff .....	6
<b>4 Caldicott Guardianship .....</b>	<b>6</b>
<b>5 Records Management .....</b>	<b>8</b>
<b>6 Subject Access Requests .....</b>	<b>8</b>
<b>7 Data Sharing .....</b>	<b>10</b>
<b>8 Information Security .....</b>	<b>10</b>
8.1 Standards and Guidance Documentation .....	11
8.2 Mobile Computing .....	11
8.3 European General Data Protection Regulation (GDPR) .....	11
8.4 Privacy Breach Detection Project .....	12
<b>9 Incident Reporting .....</b>	<b>13</b>
<b>10 Freedom of Information .....</b>	<b>Error! Bookmark not defined.</b>
10.1 Activity .....	<b>Error! Bookmark not defined.</b>
10.2 Response Times .....	<b>Error! Bookmark not defined.</b>
10.3 Reviews & appeals .....	<b>Error! Bookmark not defined.</b>
10.4 Performance monitoring .....	<b>Error! Bookmark not defined.</b>
<b>11 Training &amp; Awareness .....</b>	<b>14</b>
11.1 eLearning .....	16
<b>12 Patient Information .....</b>	<b>17</b>
<b>13 Best Value .....</b>	<b>17</b>
<b>14 Issues &amp; challenges for 2018/19 .....</b>	<b>18</b>
14.1 The Public Records (Scotland) Act 2011 .....	18
14.2 The European General Data Protection Regulations (GDPR) .....	18
14.3 Public Sector Cyber Resilience Action Plan .....	19
14.4 Raising awareness .....	19
14.5 Incident reporting .....	19
14.6 Resources .....	19
<b>Statement of Approval .....</b>	<b>19</b>
<b>Appendix 1: Information Governance Committee Membership .....</b>	<b>20</b>
<b>Appendix 2: Dates of Meetings and Attendees .....</b>	<b>21</b>
<b>Appendix 3: Incident Categories .....</b>	<b>22</b>

## Introduction

This is the eleventh NHS Borders Information Governance Annual Report and covers the financial year 2017/18 to meet the Board's Governance Reporting cycle.

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

The work is underpinned by the following:

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

With the European General Data Protection Regulation (GDPR) coming into force on 25<sup>th</sup> May 2018, a gap analysis was carried out to identify and plan for any work to make NHS Borders compliant. Having an enhanced central Information Asset Register is considered to be the key element, and a data capture system was developed to populate the Register.

The Information Governance team worked with the team implementing EMIS to replace ePEX, the Community Patient Administration System, to ensure the inclusion of Information Governance controls in the design including appropriate system use monitoring through FairWarning.

The WannaCry malware attack of May 2017 was a timely national reminder of the vulnerabilities of the digital age. Internal Audit assisted in a, what had been an already planned, review of NHS Borders cyber maturity and a number of actions from this have been incorporated into the IM&T work plan. One of the recommendations was to improve staff members' ability to recognise fraudulent emails, known as Phishing. The Information Governance team implementing a product to deliver safe Phishing emails as part of our staff awareness programme.

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 be taken up consolidating improvements in information handling that come with the imminent implementation of the European General Data Protection Regulations, and supporting the local implementation of the Cyber Resilience Plan issued by Scottish Government eHealth Division in 2017.

A handwritten signature in black ink, appearing to read 'Cliff Sharp', with a stylized, cursive script.

Cliff Sharp  
NHS Border Medical Director  
Chair of Information Governance Committee

## **1 Overview**

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

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

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

### **1.1 Information Assurance Strategy**

The national 2015 – 2017 Information Assurance Strategy is 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.

### **2.2 Information Governance Committee**

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

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

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

## **3 Policy & Planning**

### **3.1 Records Management Policy**

The Records Management Policy was reviewed by the Information Governance Lead and no changes were necessary. It was approved by the Information Governance Committee in March 2018.

### 3.2 Information Governance Policy

The Information Governance Policy was reviewed by the Information Governance Lead and minor updates were applied to reflect the new data protection legislation coming into force in May 2018. No other changes were required and the new version was approved by the Information Governance Committee in March 2018. Compliance with the policy in terms of learning and signing confidentiality statements 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. This is scheduled for Q1 2018/19.

### 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.

A large amount of time over the past 12 months has been spent on issues around the impending Data Protection Reform, the Cyber Maturity Review and subsequent Public Sector Cyber Security Action Plan.

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

- **Publishing a General Data Protection Regulation eLearning module** – This was developed by a commercial organisation and is intended for Senior Management to raise awareness of the changes in legislation.
- **Producing Data Processing Agreements** – have been issued for several projects including:
  - Alcohol Related Brain Damage project
  - Replacement dashboard for Theatre system
  - Migrating the unscheduled care service rota system, RotaMaster, to a hosted service.
- **Procuring and Implementing MetaPhish** – Sourced and implemented a product to test the 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 Code of Conduct for Staff

The NHS Borders Information Governance Code of Conduct for Staff, first published in 2011, has been further updated, along with its e-learning package. The Code of Conduct continues to be a mainstay of staff education and awareness on information governance matters.

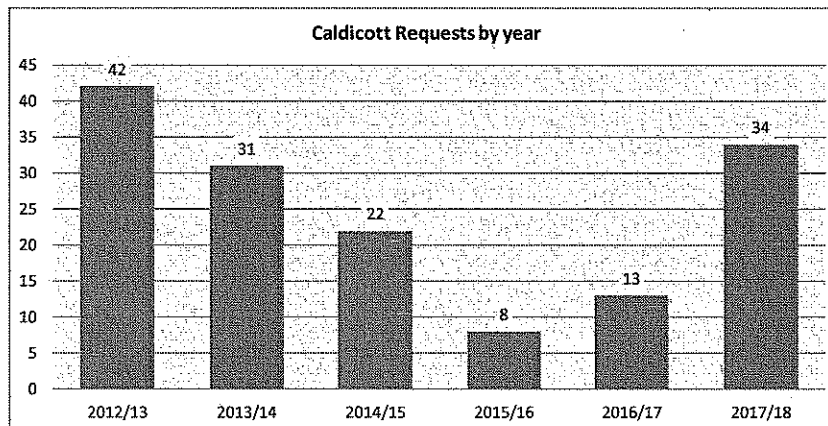
During 2017/18 the Information Governance team met with several different groups of staff to deliver awareness raising and CPD sessions. These covered various elements of the Code of Conduct dependent on the particular audience's requirements.

## 4 Caldicott Guardianship

Over the last year there were 34 applications for access to patient identifiable information which is an increase of 62% on the previous year. Most requests (85%) were from NHS Borders staff requesting access to patient records for new clinical systems such as BadgerNet and EMIS Community Web.

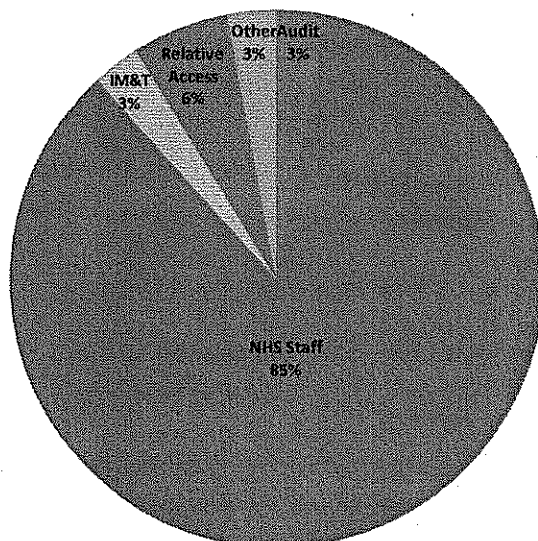
With the exception of the requests from NHS Borders there has been a significant drop in requests from other sources. This is largely due to requests being handled centrally by the Public Benefit and Privacy Panel which was set up by the Scottish Government and NHS Scotland. The Information Governance 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, 2017/18**



**Table 4.2: Types of applications received by the Caldicott Guardian, 2017/18**

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

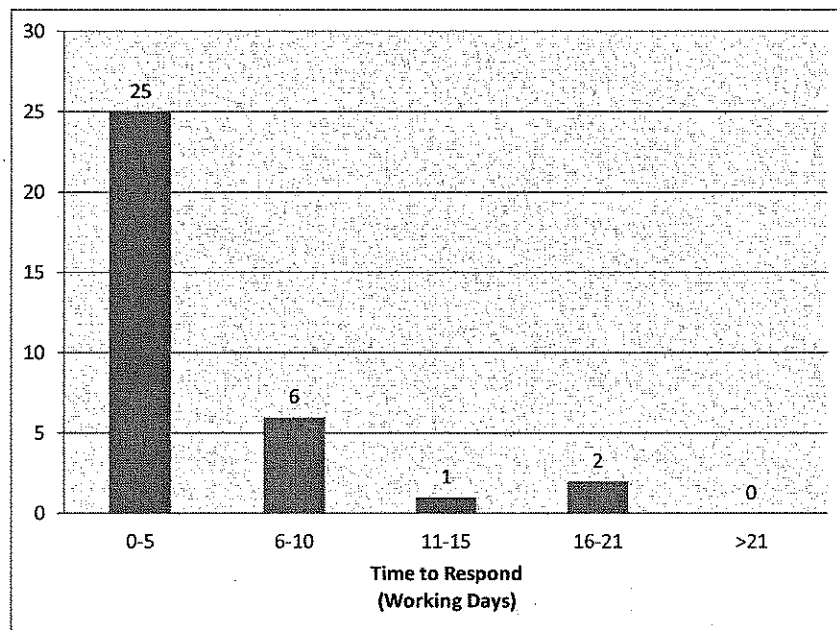


Application type	Number
Audit	1
Research	0
NHS staff Access	29
Information Governance	0
IM&T	1
Relative Access	2
Other	1
<b>Total</b>	<b>34</b>

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 but two (6%) of the applications meeting the target.

**Chart 4.1: Time to process Caldicott applications, 2017/18**



## **5 Records Management**

### **Public Records (Scotland) Act 2011**

Progress on the 2016 Records Management Plan (RMP) has been limited. This is mainly as a result of the Information Governance team concentrating on the preparatory work for the implementation of the General Data Protection Regulations in May 2018.

Work to introduce and manage an Information Asset Register has been undertaken as part of the requirements of the GDPR. This information is also necessary as part of the Business Classification Scheme for the PR(S)A and therefore effectively meets that requirement.

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.

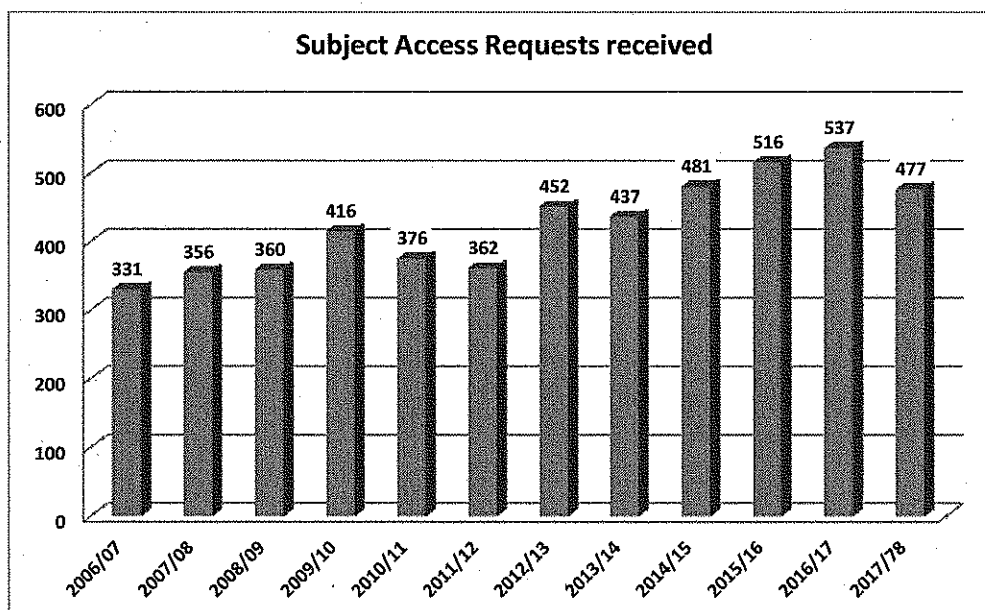
## **6 Subject Access Requests**

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

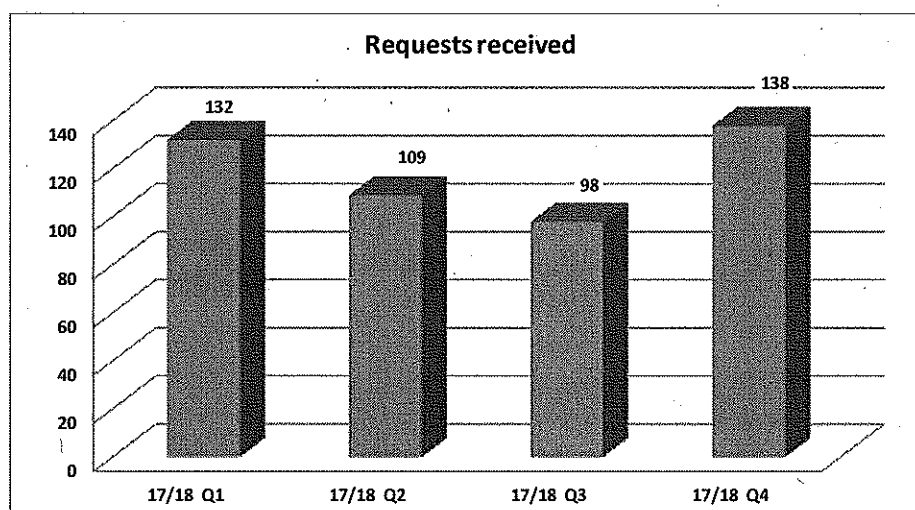
The numbers of requests received by the Subject Access team dropped off over the last 12 months. It is anticipated that when the General Data Protection Regulations comes into force in May 2018 the number of requests may rise as there will no longer be a fee charged for these.



**Chart 6.1: Subject Access Requests by Year 2006/07 – 2017/18**

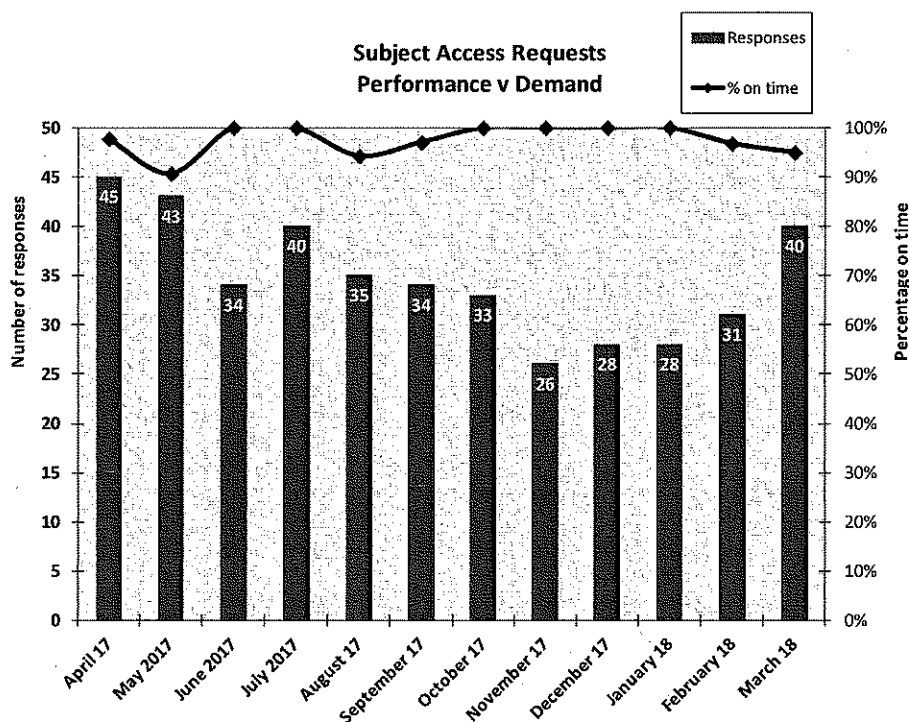


**Chart 6.2: Subject Access Requests by Quarter 2017/18**



**Chart 6.2: Subject Access Requests by Quarter 2017/18**

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 97%, an improvement of 2% from the previous year. On six occasions during the year, the monthly figures showed 100% compliance for responses.

## 7 Data Sharing

As part of the GDPR preparatory work is ongoing, to identify every type of data sharing involving person identifiable information and that suitable data sharing agreements are in place.

## 8 Information Security

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

In May 2017, NHS Borders, in common with many other NHS organisations around the UK, was affected by the WannaCry ransomware. This infected PCs in some Community locations and network shares in the BGH that those PCs connected to. The Information Governance team was involved initially in hands on patching of servers and PCs, and latterly in the subsequent Cyber Maturity review performed by Internal Audit.

Although the majority of recommendations made in the Review were of a technical nature to be addressed by IT Services, the need to improve staff awareness was also highlighted. WannaCry was not spread by malicious email; however the vast majority of exploits are performed using that medium. The Review suggested that a method to test how staff recognise and react to Phishing emails be put in place. Following a controlled Phishing test by MetaCompliance in August 2017, targeting 10% of the organisation, the Information Governance Committee agreed that a 1-year licence for their MetaPhish product could be purchased. The aim was to determine a baseline by sending out a safe, but convincing, Phish to the whole organisation and recording the actions taking by the recipients (Ignored, Opened, Clicked, Data Entered). To date, four such mails have been sent out, targeting specific departments. Whilst there have been a number of recipients clicking on the links a welcome result is the number of staff who have questioned whether the mail is genuine. This demonstrates that there is a good level of awareness of malicious emails, it is important that users are reminded of the threat that these pose.

Following the implementation of Smoothwall, the Internet web filter, several updates have taken place improving accessibility to many web pages for staff. A second installation on a virtual server is scheduled to improve availability of Internet services further by introducing failover redundancy.

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

### **8.1 Standards and Guidance Documentation**

Information Governance has a comprehensive library of standards, policies and guidance documents. Where appropriate, these are available on the Information Governance intranet page. During 2017/18 work continued to revise and update these documents in accordance with good practice guidelines.

### **8.2 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 2018/19.

### **8.3 European General Data Protection Regulation (GDPR)**

The European General Data Protection Regulations (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 20 million EUR
- 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

It should also be noted that currently the annual fee for registration with the Information Commissioner's Office (ICO) is £500. This is a statutory requirement. When the GDPR comes into force the registration with the ICO will increase to £2,900 per annum.

An essential element that must be in place in order to ensure appropriate controls are used to protect personal information is an Information Asset Register. Knowing what information is actually held by the

organisation, how it is secured and managed throughout its life cycle, including who it may be shared with, is absolutely crucial. The Information Asset Register will be used to audit the controls around each registered asset.

#### 8.4 Privacy Breach Detection Project

FairWarning remains the privacy breach detection tool used within NHS Borders and has now been in operation, providing daily reports, for 6 years.

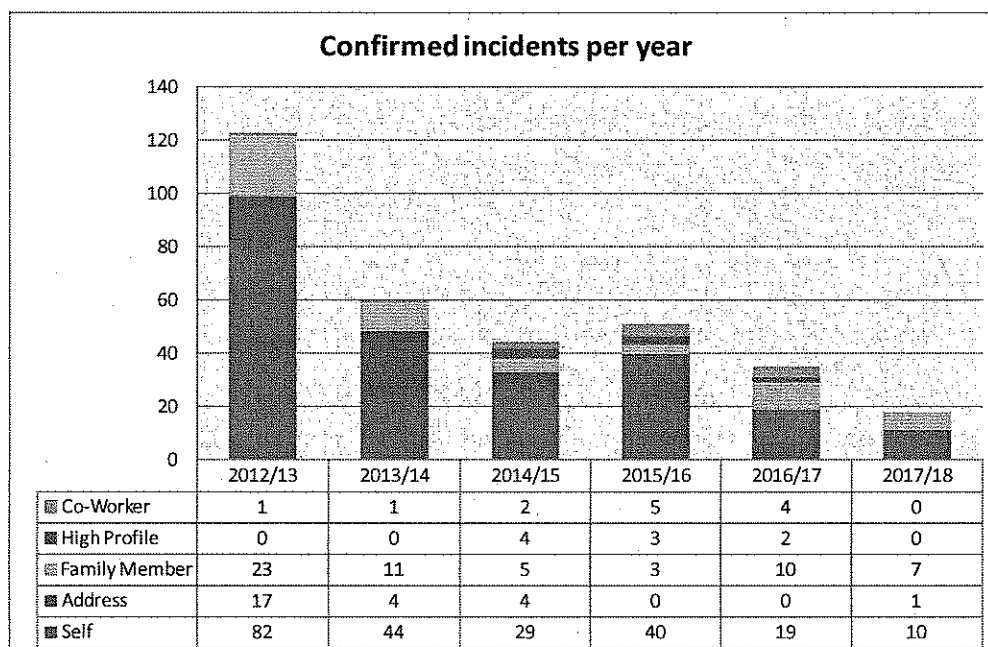
The clinical information recording systems and patient management systems used within NHS Borders log the activity of users accessing the systems. FairWarning works by importing this information on a daily basis and collates reports according to predetermined categories, such as staff looking up their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

The number of potential incidents (those where the predefined criteria were met) identified by FairWarning was down by 2% during 2017/18 on the previous year. Of the 8,405 potential incidents only 84 cases were referred to line management for further investigation. This is down 7% on the previous year. As shown in the tables below, the number of confirmed incidents was also down, by 49%, on the previous year to just 18. This represents an 85% drop in confirmed incidents since FairWarning was implemented in April 2012.

The drop in confirmed incidents could be attributed to the ongoing awareness campaign which was undertaken throughout the year. Several communications were issued via different methods (Team Brief, Staff Update, Information Governance microsite, Featured Advert, etc.).

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

**Chart 8.1: Privacy breach detection investigations and outcomes**



## 9 Incident Reporting

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

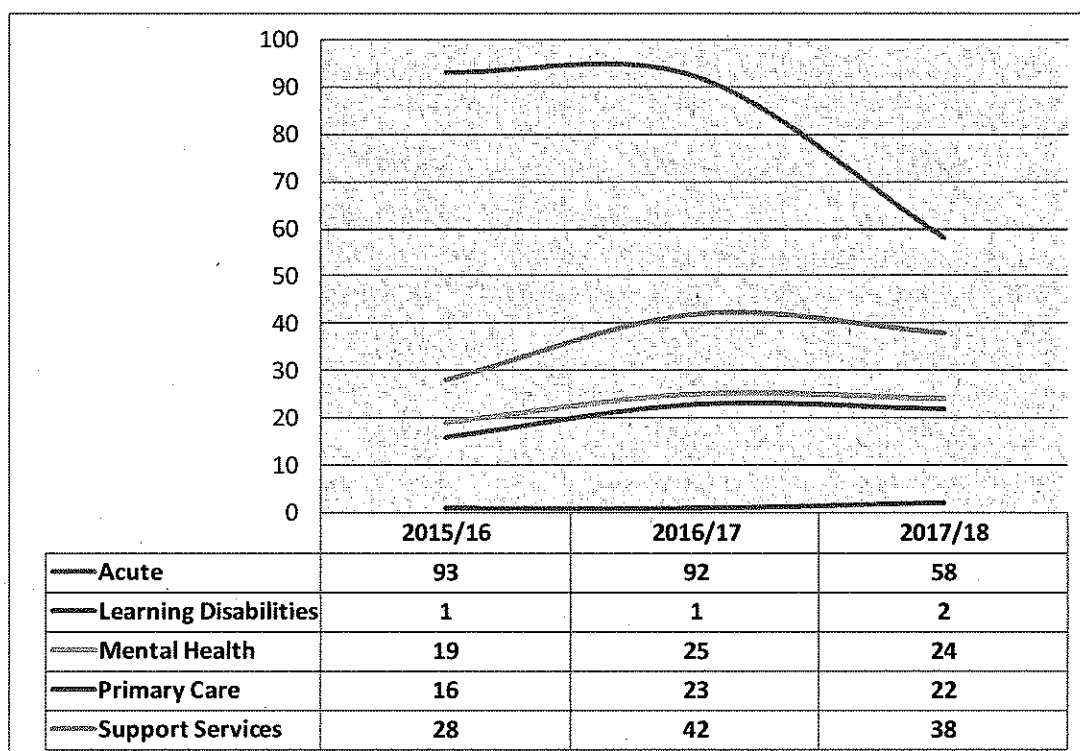
The tables below summarises the incidents reported over the past 12 months. There has been a drop in the number of incidents reported (144) compared with the previous year (183). However, this brings the number of reported incidents more in line with the previous two years. Carelessness appears to be 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 left in an inappropriate place have both recorded increased instances.

There has been a reduction in the number of incidents reported in the Acute area. This accounts for the majority of the overall drop in figures.

**Table 9.1: Summary of Types of Incident**

Incident class	Incident Summary	2015/16	2016/17	2017/18
Breach of Confidentiality	Confidential information emailed to inappropriate destination	6	6	19
	Confidential information found in public/inappropriate place	8	19	32
	Confidential information sent to wrong recipient	17	28	22
	Confidential waste left insecure	2	2	8
	Information divulged carelessly	6	13	0
	Information divulged intentionally	1	0	0
	Permitted password to be used by other person	1	1	0
<b>Breach of Confidentiality Total</b>		<b>41</b>	<b>69</b>	<b>81</b>
Failing to Secure	Confidential information emailed without appropriate security	1	2	1
	Confidential information sent but not received	2	2	1
	Hardcopy confidential information sent using inappropriate method	2	0	2
	Hardcopy confidential/sensitive data lost/misplaced/stolen	11	25	18
<b>Failing to Secure Total</b>		<b>16</b>	<b>29</b>	<b>22</b>
Inappropriate Access	Accessed clinical records without due reason (Not FW)	0	0	1
	Accessed clinical records without due reason (Not FW)	3	1	0
	Accessed family member record (FW)	2	6	5
	Accessed neighbour record (FW)	0	0	0
	Accessed other person's record inappropriately (FW)	3	4	0
	Accessed own record (FW)	32	17	10
	Accessed work colleague record (FW)	4	3	0
	Used password of other person	0	3	0
<b>Inappropriate Access Total</b>		<b>44</b>	<b>34</b>	<b>16</b>
Incorrectly filed	Patient documents/labels found in wrong record	47	39	22
	Patient documents/labels not filed at all or not in correct place in record	9	12	3
<b>Incorrectly filed Total</b>		<b>56</b>	<b>51</b>	<b>25</b>
<b>Grand Total</b>		<b>157</b>	<b>183</b>	<b>144</b>

**Table 9.2: Summary of Incidents by reporting Clinical Board**



## 10 Freedom of Information

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

Each year since its introduction, there has been 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.

### 10.1 Activity

The volume of FOI requests decreased with 2017/18 seeing a decrease of 1% on the previous year. Requests from the media continue to account for the highest volume of work at 28% with those from the Commercial sector at 26%. The Scottish Parliament accounted for 22% of the total number of request received. The other categories have all roughly stayed the same.

### 10.2 Response Times

The Act requires that all requests are responded to within 20 working days. During the year 2017/18 our compliance dropped to 96%. The main reason for this was service capacity in providing the data required to compile the responses.

The complexity, and sometimes sensitivity, of the FOI requests received can make achieving this compliance rate a challenge, one other area that can cause delays is the time it takes to get these approved and signed off for release.

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**

	<b>2017/18</b>	<b>2016/17</b>	<b>2014/15</b>	<b>2013/14</b>	<b>2012/13</b>	<b>2011/12</b>
Total number of requests responded to	617	623	527	331	399	326
Number of requests answered within 20 working days	594	619	524	243	325	292
Number of requests answered in more than 20 working days	23	4	3	88	74	34
Median number of days taken to respond	12	14	12	20	19	18
<b>Percentage compliance</b>	<b>96%</b>	<b>99%</b>	<b>99%</b>	<b>74%</b>	<b>81%</b>	<b>90%</b>

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

### **10.3 Reviews & appeals**

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

In 2017/18, one applicant requested NHS Borders undertake an internal review of the handling of their request. In this case the decision was taken to provide the applicant with further information under Section 15 of the FOI(S)A 2002 Duty to provide advice and assistance.

There were no appeals to the Office of the Scottish Information Commissioner received in this time period.

### **10.4 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 1998 not to provide data on any statistic that is less

than 5, therefore we are required to withhold under Section 38 of the FOISA. This is also in accordance with the Code of Practice for Official Statistics any number that is less than five, actual numbers and potentially identifiable information is withheld to help maintain patient confidentiality due to potential risk of disclosure. Further information is available in the [ISD Statistical Disclosure Control Protocol](#).

**Table 10.2: Outcome of requests**

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

Note: some responses fall into more than one category

## 11 Training & Awareness

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

In 2017/18, 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.

### 11.1 eLearning

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



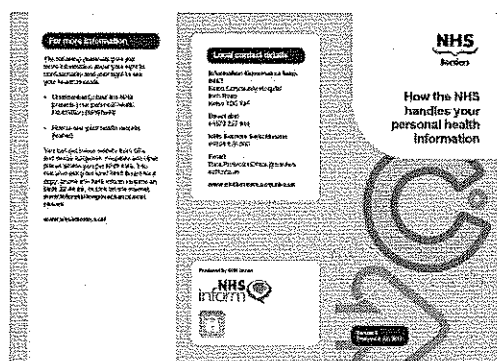
The Information Governance LearnPro training module was completely re-written and released at the end of 2016. It now relates directly to the Information Governance Code of Conduct. Staff members are required to complete this module every two years and a snapshot of figures taken on 1<sup>st</sup> March 2018 shows that 2158 out of a workforce of 3828 had undertaken this training. This represents 56% of all staff. Information Governance is one of the Board's Core Training courses and it is intended that the 'Course of The Month' programme will deliver improved compliance during 2018/19.

## 12 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.



## 13 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:

- Performed a Risk Assessment on the practice of patients transporting their own records between departments and clinics with the BGH
- Analysed the number of Subject Access Requests had been received by the Board and calculated the cost in staff time to service these requests. This will be a cost pressure when the processing fee is removed from such requests when the GDPR comes into force in May 2018.
- Trialled, and subsequently introduced, a tool to test the organisations ability to recognise and appropriately deal with Phishing emails.

- Revised IT Security and E-mail policies approved
- Revised Mobile Device policy was approved
- Revised CCTV policy was approved
- 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

## **14 Issues & challenges for 2018/19**

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 implementation of the European General Data Protection Regulations (GDPR) which will largely replace the current Data Protection Act in May 2018 will introduce changes in practice to ensure compliance over the coming year.

### **14.1 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 development 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.

### **14.2 The European General Data Protection Regulations (GDPR)**

The GDPR will come 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. Although NHS Borders is compliant with the current Data Protection Act there is still work that needs to be done, both in the lead up to May 25th and beyond, to ensure the organisation retains compliance 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 be developing and implementing 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.

#### **14.3 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 be members the team working on this in the forthcoming year.

#### **14.4 Raising awareness**

During 2017/18 the Information Commissioner took enforcement action against several health organisations in the UK for breaching data protection. This action included seven prosecutions of individuals who had accessed patient records inappropriately. 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.

#### **14.5 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.

#### **14.6 Resources**

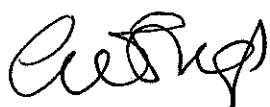
The addition of the Information Governance Officer post continues to make a significant positive impact on the workload. This post enables us to meet commitments within the eHealth strategy to strengthen IG arrangements and is funded non-recurrently from eHealth Strategy allocations. Increasing focus 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 2018. 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

30/4/18.

## **Appendix 1: Information Governance Committee Membership**

Cliff Sharp	Medical Director, Chair
Tim Patterson	Caldicott Guardian, vice chair
Claire Pearce	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
Ros Gray	Head of Quality and Clinical Governance
Vacant	Training & Professional Development
Viv Buchan	Finance
Vacant	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

### June 2017

Meeting Cancelled

### 14 September 2017

Dr Cliff Sharp	Medical Director (Chair)
Tim Patterson	Caldicott Guardian
June Smyth	Director of Workforce & Planning, SIRO
Jackie Stephen	Head of IM&T
George Ironside	Senior Health Information Manager
John McLaren	Area Partnership Forum representative
Viv Buchan	Senior Finance Manager
Anne Palmer	Clinical Governance and Quality (for Ros Gray)

#### In attendance:

Julie Dickson	Information Governance Officer
Carol Graham	Freedom of Information
Jill Bolton	Minutes

### 11 December 2017

Dr Cliff Sharp	Medical Director (Chair)
Tim Patterson	Caldicott Guardian
George Ironside	Senior Health Information Manager
Ros Gray	Head of Clinical Governance and Quality

#### In attendance:

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

### 30 March 2018

Dr Cliff Sharp	Medical Director (Chair)
Tim Patterson	Caldicott Guardian
George Ironside	Senior Health Information Manager
Kim Carter	Senior Finance Manager
Jackie Stephen	Head of IM&T

#### In attendance:

Ian Merritt	Information Governance Lead
Carol Graham	Freedom of Information
Keith Allan	Public Health, shadowing Tim Patterson
Jill Bolton	Minutes

### Appendix 3: Incident Categories

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

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

