South Eastern Health and Social Care Trust

Information Governance Annual Report 2018/2019

As Director responsible for Information Governance (IG) and as the Senior Information Risk Owner (SIRO) for the Trust, I am pleased to present the annual report on the Trust's Information Governance arrangements for the 1 April 2018 to 31 March 2019. Key areas of information governance include confidentiality, data protection, records management, freedom of information, information security and cybersecurity.

IG within the Trust provides a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards, in a modern health and social care service. Employees must be able to deal with the many different information handling requirements, relating for example, to patients, clients and staff. The Trust aims to safeguard patient/client confidentiality and maintain data security whilst empowering staff to perform their role using key information governance principles.

With the introduction of the General Data Protection Regulation (GDPR) and the updated Data Protection Act in May 2018, the penalties for breaking data protection and associated laws are now significant.

I would like to record my thanks and appreciation to the Information Governance Department for all the preparatory work required to ensure smooth transition to the new Regulation.

Myra Weir
Director of Human Resources & Corporate Affairs /
Senior Information Risk Owner

Key Facts & Figures for 2018/2019

Subject Access Requests (SARs)

- 4,543 SARs received for access to records
- 85% of SARs processed within legal timeframe.

FOI Requests & Enquiries

- 423 requests/enquiries received
- 84% of requests/enquiries processed within legal timeframe.

IG incidents

- 219 - IG incidents were recorded on Datix
- 7 - IG incidents were reported to the ICO.

IG Training

- 4 different IG related training courses were provided by IG staff
- 1,377 staff completed mandatory data protection training
- 171 senior staff attended GDPR awareness sessions.

DPIAs Approved

- 11 Data Protection Impact Assessments (DPIA) were approved.

DAAs Approved

- 35 Data Access Agreements were approved.

ICO Communications

- One complaint received from the ICO in relation to how information was being handled, the Trust's decision was upheld by the Information Commissioner.

Information Governance Structure

The Information Governance Steering Committee (IGSC) is a sub-committee of the Corporate Control Committee. Its role is to oversee the IG strategic agenda and it also has a responsibility to lead and foster a culture that values, protects and uses information for the public good. The IGSC continued to roll-out a challenging programme of work during the year, primarily based around the embedding of GDPR across the Trust.

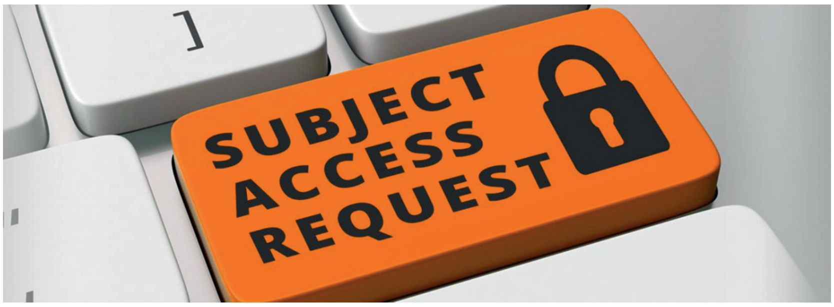
The Trust has appointed a SIRO and a deputy SIRO (Mrs M Weir and Ms R Coulter), 2 Personal Data Guardians (Mr CJ Martyn, Mrs B Mongan [formerly Mr B Whittle]), a Chief Clinical Information Officer (Dr D Wilson) and a Data Protection Officer (Miss L McAree). Within the Trust there are 34 nominated Information Assist Owners (IAOs) who are at Assistant Director level. They are supported in their role by Information Asset Assistants (4th level management tier).

New Legislation

The General Data Protection Regulation (GDPR) which forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018) came into force on the 25 May 2018. This legislation will continue to be enforced after the UK's exit from the European Union. The Trust has a statutory responsibility to know what personal data it holds, how and why it is processed, who has access to it, and with whom it is shared.

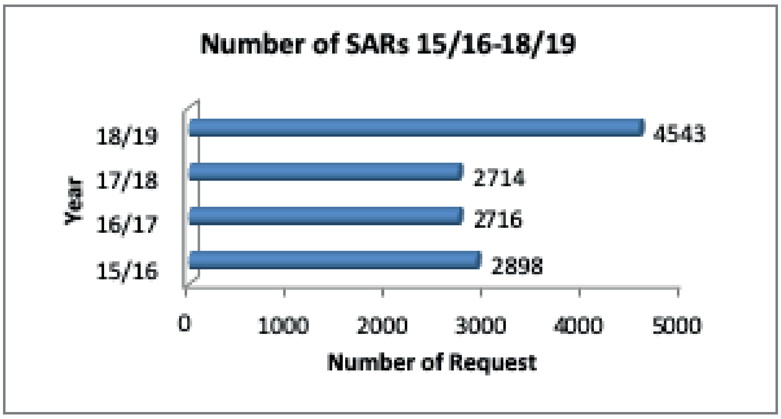
The Trust worked as part of a regional subgroup of the Health & Social Care (HSC) Information Governance Advisory Group (IGAG) to develop and implement an action plan to meet the requirements of the new Regulation. Many resources, such as privacy notices, patient/client leaflets and staff training, were developed in collaboration with all the Northern Ireland (NI) HSC Trusts. The Trust trained over 171 senior managers in preparation for the new legislation. Key impacts for the Trust include:

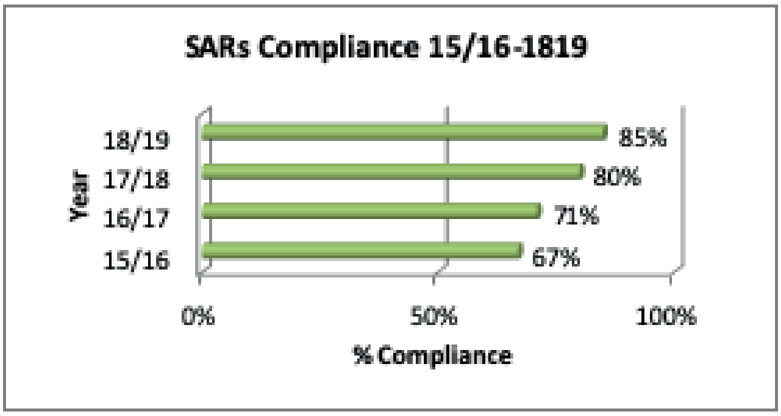
- Reporting IG incidents to the ICO within 72 hours
- Completion of Subject Access Requests (SARs) to be within 30 days, or 90 days where the request is complex
- No income generation now as all SARs are free
- New projects, systems or processes must have a data protection impact assessment (DPIA) completed
- Contractual documentation more detailed with respect to data flows
- All staff must attend mandatory data protection training
- Information assets to be documented by the Trust.



Subject Access Requests (SARs)

A key part of data protection legislation allows individuals to request a copy of any personal information we hold about them. The number of SARs received by the Trust increased by 39% in 2018/2019. This may be attributed to the implementation of the GDPR and heightened national awareness and publicity campaigns associated with promoting citizens' rights and the removal of fees. The majority of requests are received from individuals or their advocates.





The Trust is legally obliged to respond to SARs within a defined time period, ie. within a calendar month for routine cases, or if the request is complex, this can be extended by a further two months. A complex case is defined regionally as a request that *"crosses one or more services, involves more than one volume/file of records, requires retrieval from hybrid systems, ie. manual and electronic, requires redaction or pertains to historical information".*

SARs received by the Trust, particularly requests relating to family and child care and social work records, are generally considered complex. These records require review and redaction and due to the complexities of the work involved, delays in issuing records have incurred. During the year both the IG and Children's Services have piloted new ways to manage this work to make it more patient/client focussed. To date the pilot outcomes have been very encouraging.

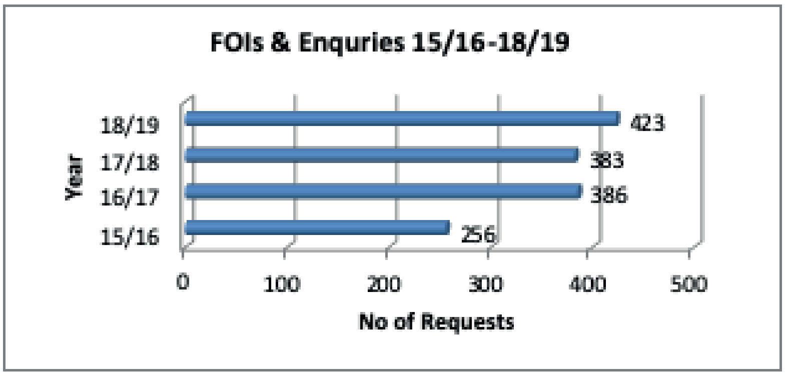
Despite the 39% increase in activity, compliance rates have increased to 85%, a 5% improvement on the previous year. Over a 4 year period requests have increased by 57%.

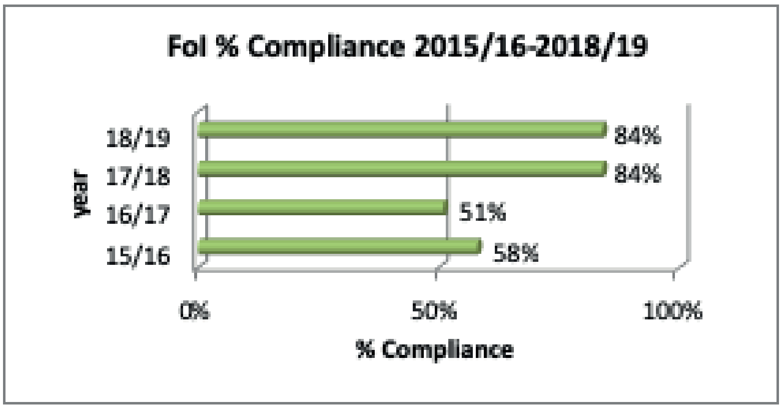
Police requests (Form 81) for the year are recorded as 70; however it would appear there has been under-recording of Form 81 requests across the Trust.

Freedom Of Information Requests (FOI)

Under the FOI Act individuals have a legal right to access information held by the Trust, subject to certain conditions and exemptions contained in the Act.

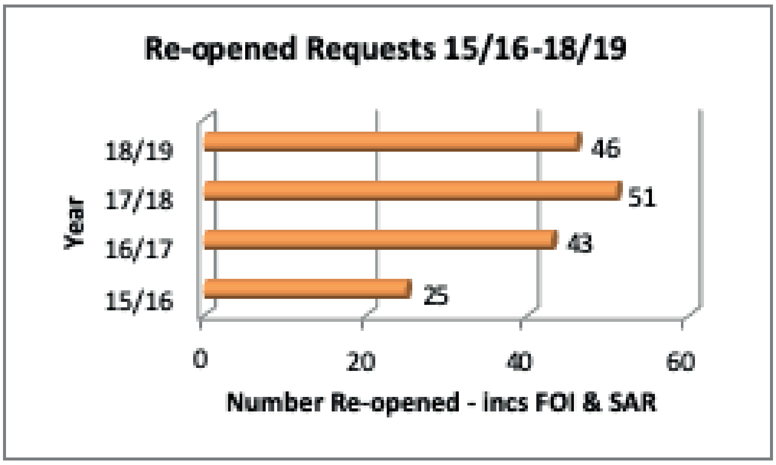
The volume of FOIs received by the Information Governance Department averaged 32 per month with a large volume of requests coming from the media, whatdotheyknow.com and commercial organisations. This is consistent with previous years. With regard to trends identified in the requests received, a significant number of FOIs relate to contract expiry dates, incident management and reporting, services provided in the community, activity management across the acute sector and staffing levels and reliance on locum and agency staff across disciplines and the associated costs.





Whilst there was a 7% increase in FOI activity during 2018/2019, compliance rates remain static at 84% when compared with the previous year. Over a 4 year period, FOI requests increased by 65%.

A total of 46 requests were re-opened during the year, as the requester was dissatisfied with the response or sought further clarification in respect of their initial request. There was a slight decrease on the number of re-opened cases in comparison with previous year.



How well did we do?

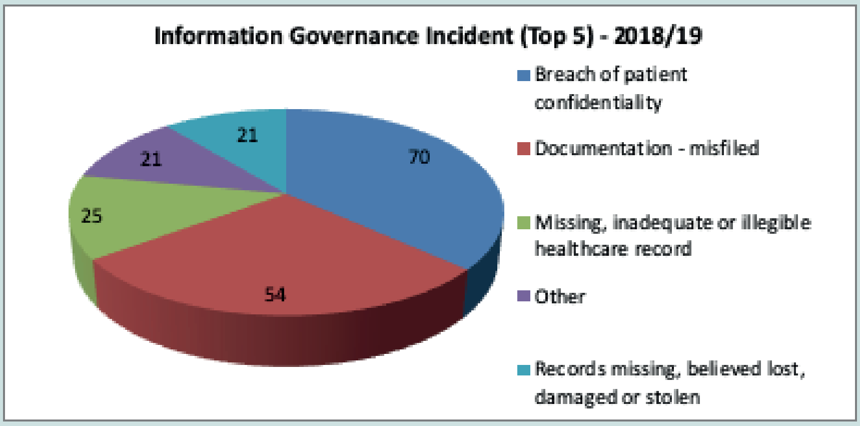
The Information Commissioner's Office (ICO) refers cases to the Trust if complaints have been received from members of the public. In 2018/19 one case was submitted for investigation to the ICO. The outcomes for the period 2015/16 - 2018/19 are summarised below:

Data Protection complaints	Complaints Received	Complaint Upheld	Complaint Not Upheld*	Request to take action
15/16	7	1	6	Yes
16/17	3	-	3	No
17/18	6	-	6	No
18/19	1	1	0	Yes

*Agreed with Trust actions

IG Incidents

Within the new GDPR legislation, the Trust is required to report any personal data breach that is likely to *"result in a risk to the rights and freedoms of natural persons"*. Throughout the year 219 IG breaches were recorded. This represents 1.1% of all incidents recorded by the Trust. Many relate to breaches of service users' confidentiality caused by inappropriate handling of personal data, eg. mis-sent emails, information sent to wrong individual, etc.



Many of the IG breaches did not reach the criteria for reporting to the ICO. However, since the introduction of the GDPR there has been an increase in the number of data breaches reported to the ICO compared to other years. The ICO has closed all cases and commended the Trust for its prompt internal remedial actions.

Data Breaches reported to the ICO by year				
2014/15	2015/16	2016/17	2017/18	2018/19
2	3	0	4	7

There is a clear requirement to ensure all staff are aware of the need to report any data breach to the information governance office as soon as possible. Only 29% (2) of cases were reported to the ICO within the legal timeframe of 72 hours. Remedial actions have been taken to improve this situation.

The **7** incidents were reported to the ICO for the following reasons

4 Incidents - **Breach of Patient Confidentiality**

1 Incident - **Consent, Confidentiality or Communication**

1 Incident - **Missing, Inadequate or Illegible Health Record**

1 Incident - **Records missing, believed lost, damaged or stolen.**

Learning from incidents is regularly published through IG Awareness updates and the Information Governance Steering and Lessons Learnt Committees. Examples will also be incorporated into the mandatory data protection training.

Information Governance Training

Data protection training is mandatory within the Trust and can be taken online, in classroom or as customised training. The IG e-learning module has been revised in accordance with the requirements of GDPR. A data protection video was also launched in January 2019. As at 31 March 2019, figures indicate that the uptake for Information Governance training is 79%.

Organisational Controls Assurance - Information Governance

In 2018/2019 the Department of Health (DoH) introduced a new annual assurance programme for HSC organisations which included a standard for Information Management (IM). HSC organisations are now required to maintain the best practice standards set out in the guidance document in order to be able to both provide assurance to the DoH and for BSO Internal Audit purposes. BSO Internal Audit will continue to audit HSC organisations' IM compliance on a periodic basis. The Trust was subject to an IM audit in November 2018.

The resultant audit report provided the Trust with limited assurance in relation to Information Governance GDPR compliance. It was stated that *"Whilst providing limited assurance it is clear that the Trust has taken proactive steps to prepare for GDPR ie. governance structures have been established, actions plans developed and monitored, Data Protection Officer appointed, privacy notices developed, lawful basis determined and guidance developed to ensure appropriate Data Protection Impact Assessments.*

Limited assurance is provided on the basis that work is needed to review, re-design and implement mechanisms to identify all information assets owned by the Trust."

The Trust has developed an action plan to take this work forward during 2019/2020. The IGSC will oversee and monitor the progress of this action plan.

In addition, the Trust's Information Governance & Information Technology & Telecommunication Departments undertook a joint audit of information systems in line with Internal Audit's recommendation (2014). Five systems were audited, and all recommendations raised through this audit have been addressed.

Each Directorate holds an extant information asset register and, in accordance with the IGSC's programme of work, each Directorate ensures that information risks are considered in conjunction with the Trust's Risk Management Strategy.

The Trust's Information Governance Department has also worked closely with the DoH and the Trust's Business Continuity Department in respect of preparation for a No Deal Brexit and the associated data protection implications.

The Information Governance Department as part of the Risk Management & Governance Directorate was re-accredited as Investors in People (IiP) compliant, February 2019 and retains ISO accreditation.

Information Quality

The Trust has a strong focus on data quality and its importance for patient safety.

The central training team work closely with information management teams and information technology colleagues to provide support and guidance to staff that are based across acute and community areas.

Within clinical coding area, performance is best in the region. Performance is 100% against the standard “Clinical Coding to be completed within 3 months of discharge”. The number of clinical codes applied to an episode of care is a key indicator of coding quality. During 2018/2019 the average number of codes applied by the Coding team was 5.3 against a regional average of 4.8.

The information teams across acute and community areas provide regular data quality reports to service areas and data quality is monitored on a weekly basis. The Trust is also utilising Qlik software to identify data anomalies in real time.

Health and Care number coverage for 2018/2019 was maintained at 99%.

The Trust continues to focus on data quality and its importance for patient safety. The Performance and Information team are working closely with the regional Data quality group that reports to the regional Information Standards Board to monitor data quality and take necessary steps to continually improve. The Trust has been involved in the production of the first annual regional data quality report and works with the regional team to address key areas of concern via a regional work plan. This includes work with groups such as the demographic improvement group, the data standards working group and the expediting of implementation of regionally agreed technical guidance across all its sites. It is recognised regionally that data quality requires a continual focus and increased resources to deliver sustained and improved data quality. It is anticipated the appointment of the regional Chief Digital Information Officer (CDIO) will promote this work as a part of the digital strategy to be developed. Processes are in place to highlight areas for data quality improvement and to avoid errors occurring at source.

ICT & Cybersecurity

The Trust is aware of the international risk of cybersecurity. Increased awareness has been a priority, and on 23 April 2018 a business continuity exercise entitled Siberia, was undertaken. This was a major desk-top exercise to test the resilience of plans and was widely supported by all professions across the Trust. As a result of this exercise, the Trust’s Corporate Business Continuity Plan has been reviewed.

Cybersecurity remains on the Corporate Risk Registar.

Regional / Partnership Working

The Head of Information Governance participates in a number of regional groups including: Information Governance Advisory Group, NI Electronic Care Record Information Work stream, Cybersecurity Programme Board, Annual Privacy Advisory Group and the IG Network Group.

Collaborative working with other Trusts has led to the shared development of a number of resources:

- Regional privacy notice, information, posters
- Data Access Agreement (DAA) template
- Data Protection Impact Assessment templates
- SAR protocol
- Regionally agreed DAA for specific projects, eg staff survey, cancer survey.

Collaborative working with internal/external stakeholders:

- Contract Advisory Groups (CAG's) to ensure appropriate updated data protection requirements, post GDPR
- Data Protection Impact Assessments (DPIA) review and guidance.

Looking Forward 2019/2020

- To progress recommendations outlined in the Information Management audit report – this is primarily around the review and redesign of the Trust information asset register and is being taken forward on a regional basis
- Continued involvement in diverse Trust/Regional initiatives/projects such as Smart4Hearing, Cultural Assessment Tool (CAT), SBNI Project for Prison Healthcare and Deprivation of Liberty Safeguards
- Continued partnership working between the Information Governance and Family & Child Care Departments to improve the service user's experience for access their records
- Follow up work in preparation for the ICO training audit revisit (August 2019)
- To design and deliver additional Information Governance training packages, eg. How to manage subject access requests (SAR), Information Governance Awareness and Redaction training
- Continued embedding of the SAR process across the Trust
- IG staff to undertake accredited training to equip them professionally for their role
- Implement new software technologies to assist IG staff in processing requests for information.

Information Governance
Lough House, Ards Hospital, Church Street, Newtownards, BT23 4AS
T: (028) 9151 2201 E: informationgovernance@setrust.hscni.net