NHS 24
BOARD

27 AUGUST 2020
ITEM NO. 6.2.6
FOR APPROVAL

INFORMATION GOVERNANCE AND SECURITY ANNUAL REPORT 2019-20

Executive Sponsor:	Chief Information Officer
Lead Officer/Author:	Head of Information Governance & Security & DPO
Action Required	This report is presented to the Board for their approval.
Key Points for this Group to consider	The paper provides an overview of the key areas of activity for the period 2019/20 for the Information Governance and Security team in ensuring compliance with all legislative requirements. Included in the report, are a number of key points including; • Network Information System Regulations • Training • Incidents
Governance Process	This paper was presented to the Audit and Risk Committee and the Planning and Performance Committee in August 2020.
Key Risks	This paper does report directly on specific risks, however the reporting and governance exercised may have an impact on IG&S risks e.g. those related to Information Asset Owners and Cyber Security.
Financial Implications	There are no direct financial implications arising from this report for 2019/20, though work reported here may result in the request for financial support.
Equality and Diversity	There have been no equality and diversity issues identified arising from this report.

1. RECOMMENDATION

1.1 The Board is asked to approve this report which provides assurance on the Information Governance and Security activity for the period 1 April 2019 to 31 March 2020.

2. TIMING

2.1 This report sets out the activity of the Information Governance and Security team for 2019/20 for assurance at the Planning and Performance Committee in August 2020.

3. BACKGROUND

3.1 This report forms part of the assurance process on the effectiveness and completeness of Information Governance and Security activity for the period 1 April 2019 to 31 March 2020.

3.2 The team continue to work conscientiously to ensure handling of information within NHS 24 is done in accordance with the following legislation and guidance frameworks:

- Data Protection Act 2018
- General Data Protection Regulation
- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations 2004
- Public Records (Scotland) Act 2011
- Access to Medical Records Act 1988
- Access to Health Records Act 1990
- Children and Young People (Scotland) Act 2014
- Computer Misuse Act 1990
- Digital Economy Act 2017
- The Privacy and Electronic Communications Regulations 2003
- The Network and Information Systems Regulations 2018 (NISR)/EU Network and Information Systems Directive (NISD)
- Common Law Duty of Confidentiality
- Caldicott Principles

4. AREAS OF FOCUS

4.1 The Information Governance and Security Team focussed their work on a number of key areas during the period of this report:

- Data Protection
- Freedom of Information/Environmental Information
- Information Security
- Policies, Procedures and Protocols
- Records Management
- Data Protection Legislation (Including GDPR)
- Network and Information Systems Regulations
- Training

- Incidents

4.2 Data Protection

4.2.1 As a Data Controller pursuant to the Data Protection Act 2018 (DPA) NHS 24 is required to deal with Data Subject Access Request (DSARs) from individuals who wish to know (and gain access to) the personal information that NHS 24 holds on them. The activity for the period of this report is shown, with 2018/19 as a comparison in the table below.

	2019/20		**2018/19**	
Patients/NoK/Parent/Solicitor	111	46%	107	41%
Police/PF/CR/CI	92	38%	99	38%
Partners	4	2%	4	2%
Staff	25	10%	30	11%
Social Work	0	0%	4	2%
GMC/CLO/NMC/SPSO	8	3%	9	3%
Nursing Homes	1	0%	2	1%
Others	3	1%	6	2%
Total	**244**		**261**	

4.2.2 The number of DSARs has been broadly consistent between last year and this. The requests under 'Other' were from the Inverclyde Council fraud dept., Disclosure Scotland and the National Crime Agency.

4.3 Freedom of Information/Environmental Information

4.3.1 The Information Governance and Security Team coordinate requests for information under the Freedom of Information (Scotland) Act 2002 (FOISA) and the Environmental Information (Scotland) Regulations 2004 (EIRs). The number of requests for the year are shown below with 2018/19 as a comparison. This report provides additional information regarding the FOI and EIR releases.

	2019/20	**2018/19**
No. of FOI Requests	112	119
No. of EIR Requests	2	0
No. of Invalid Requests	9	0
Of responses issued no. of On Time Responses	112	111
Of responses issued no. of Late Responses	2	8
Of responses issued no. of Full Release	23	19
Of responses issued no. of Partial Release	22	25
Of responses issued no. of Information Not Held	30	34
No. of requests closed because of no clarification	1	1
No. of requests withdrawn by requester	5	5
No. of Reviews	3	5
Repeat Requests	1	3
Personal Information	16	28
Refusal – handled as EIR	1	0

Otherwise Accessible	5	3
Intended for future publication	1	0

4.3.2 The number of requests is broadly similar to last year. As the requests can come from anyone anywhere in the world it is difficult to predict the number and nature of them. The invalid requests were missing a description of the actual information being requested or because the name of the requester was not included. Whilst incomplete requests are a technical element of the Act it renders the request invalid and one which the Scottish Information Commissioner would likely not consider under appeal.

4.3.3 The team had been disappointed in the 8 late responses in 2018-19 and had set the target of zero late responses this year. As can be seen from the table there were 2 late responses this was due to requests being received into a non IG&S generic mailbox where they remained for a period of time. The delay in passing them to the IG&S team meant the requests were already late when they were passed to the team. That situation was reviewed and addressed with those responsible for the management of the generic mailbox.

4.3.4 As is consistent across the years the majority of the requests were received from members of the public. A breakdown of request sources is shown below:

Source of Request	**No. Of Requests**
Internal	3
Press	3
Public	72
MSP/MP/Local Councillor	7
Commercial Organisation	23
Other	6

4.3.5 For this report the items classified as ‘Other’ were from a solicitor, Police Scotland, a territorial Health Board, the British Medical Association (BMA), Scottish Government and a Trade Union.

4.4 Information Security

4.4.1 Information Security focuses on three main principles; the confidentiality, integrity and availability of NHS 24 information. There is a requirement to ensure that these three principles are applied to the control of all NHS 24 information.

4.4.2 To identify and assess risks to the systems an assessment called a System Security Policy (SSP) is produced and goes through a two tier review process. Over this year this process has not been as successful as we need it to be, so it is undergoing a review to understand what improvements can be made.

4.4.3 A number of Information Security activities have taken place during the period of this report, these included:

- The installation of updated CCTV equipment across the estate to replace equipment which was out of support. It is hoped that more of the legacy

equipment can be replaced through 2020/21 to ensure that it is fit for purpose.

- The upgrade of the central control solution for the anti-malware system was completed. During 2020/21 it will be reviewed in conjunction with the national anti-malware direction of travel.
- The deployment of a replacement web filter product was largely successful which has improved the security posture of the estate. There remains work to be done to modify and simplify legacy set-up to fully realise the benefits of this new system.
- The upgrade of the badge access control system has seen all legacy controller hardware replaced with the migration to the new environment commencing in early 2020/21.
- A successful review of the legacy PRM system has resulted in a 48% reduction of access rights.
- A cyber security audit was undertaken by the internal auditors, the report from that audit has been provided and an action plan will be developed based on that report.

4.5 Policies Procedures and Protocols

4.5.1 A number of policies were reviewed throughout the year, though this activity was, at times, de-prioritised because of other work pressures and commitments. A number of policies remain to be reviewed and this will be undertaken with a raised priority level to ensure they are completed.

4.5.2 New procedures for existing operations such as the DSAR process have been put under test though those tests have now been accelerated by the current pandemic. The results and final decisions on that procedure will be reported on in future IG&S reports.

4.6 Records Management

4.6.1 Throughout the year a number of record management sessions including 1-to-1 and training have been delivered across the organisation. These sessions have seen an improvement of a core element - from both a records management and a data protection perspective – which is the Information Asset Register (IAR). Whilst it has seen improvement there is still scope for this to be further improved and this work will continue through 2020/21.

4.6.2 The training that has been delivered includes both online eLearning and face to face, those face to face sessions have been targeted sessions for:

- The Information Asset Owners (IAOs)
- The Information Asset Administrators

4.6.3 The policy compliance system was successfully used to deliver the Declaration of Responsibilities to the IAOs this provided evidence to complete an outstanding internal audit action.

4.6.4 During the course of the year a volume of historic paper records were identified for destruction, this included personal and corporate information. This highlights how important good records management practices are because the exercise to destroy the records meant that they were no longer

subject to either a data subject access or a freedom of information request. It also meant that NHS 24 were no longer paying for those records to be stored off site.

4.6.5 An essential piece of work which started during the period of this report is on the identification of the data which will be transferred to Microsoft SharePoint as NHS 24 migrates to Microsoft Office 365. Though in progress, a significant amount of work is still required for this to ensure that the appropriate information is migrated and therefore available for use by staff who may no longer have access to network file shares.

4.7 Data Protection Legislation (including GDPR)

4.7.1 A GDPR compliance review was carried out by our internal auditors. The resulting report highlighted only low rated recommendations, though the conclusion was Reasonable Assurance based on an outstanding action (rated medium) from a previous audit which also had an outstanding low rated item.

4.7.2 This year has seen the closure of two internal audit actions which have been outstanding since the previous audit. One which was rated as low, the other as medium. Evidence for the completion of both was accepted by the internal auditors which has allowed for them to be closed.

4.7.3 The recommendation from the internal audit compliance review for additional resource within IG&S is being considered, a job description for a Deputy DPO/IG Manager has been drawn up.

4.7.4 The risk assessments done as Data Protection Impact Assessments (DPIAs) have been an area of contention throughout the year. The process has been reviewed and further enhancements in the form of an electronic system will be delivered. This system has been procured in conjunction with a number of NHS Scotland Boards and is in the process of final configuration with implementation expected in 2020/21. This process also involves a two tier approach and throughout the year the Tier 1 Panel has seen changes including the introduction of other members of staff as members of the panel such as staff side representation because the DPIA is an assessment of risk to the personal data of the data subjects, those data subjects also include NHS 24 staff.

4.8 Network and Information Systems Regulations

4.8.1 As an Operator of Essential Services (OES) NHS 24 is subject to the UK implementation of the Directive which is the Network and Information Systems Regulations 2018. To comply with the Regulations an updated NHS Scotland Security Policy Framework has been produced.

4.8.2 Elements of the above framework and the National Cyber Security Centre 10 Steps plan were used by the Internal Audit staff as the scope for the Cyber review. It is expected that there will be a number of findings from this internal audit review which will be welcomed as opportunities for improvements. The audit took place in Q4 and an action plan will be developed from the audit report.

4.8.3 NHS 24 will also be subject to audits from the NIS Regulator which has been formed by Scottish Government as the Health Competent Authority (CA). As

NHS 24 were subject to the internal audit in Q4 the Health CA have determined that their audit will be towards the end of 2020 to allow any internal audit findings to be implemented prior to their review.

4.9 **Training**

4.9.1 There were a limited number of opportunities for team members to pick up some level of training on Office 365 at a security workshop and a records management workshop provided by Microsoft. These events have highlighted the need for additional training on this as the changes are significant.

4.9.2 Both internal and external sessions were delivered on DPIAs and it is hoped that additional external sessions may be delivered through 2020/21 as improvements for the understanding and production of the DPIAs.

4.9.3 An external Records Management Practitioner training course was organised by the team which was set-up to allow other NHS Scotland Boards to attend. The set-up was well received with the requests from the Boards exceeding the number of available spaces. The course is split across a month with the first half being delivered but the second half being delayed because of the current pandemic situation.

4.9.4 The team have also delivered a number of sessions across their areas of responsibility including:

- Information Asset Ownership
- Appropriate redaction of data subject access requests
- Completion of information asset register entries
- The Freedom of Information process
- Introductory and overview training on both the role of the IG&S team and Data Protection in general.

4.9.5 There is a requirement for all NHS 24 staff to undertake mandatory Information Governance eLearning training which is available on Turas Learn. The team worked with the L&PE department on this and are producing reports which are provided to the Information Asset Owners and included in IG&S quarterly reports. This will continue throughout 2020/21.

4.10 **Incidents**

4.10.1 As part of the regulatory regime that NHS 24 operates within, an incident which has resulted in a breach of either the Data Protection Legislation or the NIS Regulation must be considered and assessed against certain criteria. If the incident is considered to have met the criteria then it must be reported to the relevant competent authority. If the incident does not meet those criteria it must still be logged but does not require to be reported to the competent authority. As the IG&S Team are also responsible for physical security then a physical security incident is also recorded.

4.10.2 There were a number of incidents which occurred during the period of this report, these included:

- The suspected theft of equipment from a centre, this was reported to Police Scotland and lessons have been learned from this.

- A redaction and misfiling issue which was deemed to be a reportable incident and reported to the ICO with no further action.
- A report template issue which was deemed to be a reportable incident and reported to the ICO with no further action.
- An email misdirection issue was deemed to be a reportable incident and reported to the ICO with no further action.
- An outage on a national system caused an issue for NHS 24 which required a level of contingency to be invoked, this was deemed a reportable incident and reported to the Health Competent Authority.
- An issue with the SAP system which resulted in a delay in completing or saving calls resulted in a level of contingency being invoked, this was deemed to be a reportable incident and reported to the Health Competent Authority.

5. FINANCIAL IMPLICATIONS

5.1 There are no direct financial implications from this report, though it is expected that there will be financial implications form the 2020/21 work plans and for improvement works such as possible data loss prevention solutions and continuing Data Protection Legislation and NISR works.