Annex B

Health Group Internal Audit

Reference number: DHX 217 008 002
FINAL REPORT
HUMAN FERTILISATION & EMBRYOLOGY AUTHORITY
SEPTEMBER 2017

Report Name:
Data Loss

Overall report rating: MODERATE

Health Group Internal Audit part of Government Internal Audit Agency (GIAA) provides an objective and independent assurance, analysis and consulting service to the Department of Health and its arms length bodies, bringing a disciplined approach to evaluating and improving the effectiveness of risk management, control and governance processes.

The focuses on business priorities and key risks, delivering its service through three core approaches across all corporate and programme activity:

- Review and evaluation of internal controls and processes;
- Advice to support management in making improvements in risk management, control and governance; and
- Analysis of policies, procedures and operations against good practice.

Our findings and recommendations:

- Form the basis of an independent opinion to the Accounting Officers and Audit Committees of the Department of Health and its arms length bodies on the degree to which risk management, control and governance support the achievement of objectives; and
- Add value to management by providing a basis and catalyst for improving operations.

For further information please contact:
Cameron Robson - 01132 54 6083
1N16 Quarry House, Quarry Hill,
Leeds, LS2 7UE

CONTENTS PAGE

1. Executive Summary 1
2. Review Conclusion 1
3. Summary of Findings 2
4. Next Steps 2
5. Recommendations Table 3
6. Detailed Findings 4

Date fieldwork completed:	10/08/2017
1st draft report issued:	15/09/2017
Management responses received:	25/09/2017
2nd draft report issued:	N/A
Management responses received:	N/A
Final report issued	25/09/2017

Report Author: Kashem Ali
Version №: Final

Distribution List – Draft Report

Main recipient(s)

Nick Jones	Director of Compliance and Information

cc:

Jeremy Nolan	HFEA Head of Audit
Tony Stanley	Audit Manager
Cameron Robson	Group Chief Internal Auditor

Distribution List – Final Report

As for draft report and:

Morounke Akingbola	Head of Finance
Richard Sydee	Director of Finance and Resources

EXECUTIVE SUMMARY

1. Introduction

1.1. The Human Fertilisation & Embryology Authority (HFEA) is the regulator of fertility treatment and human embryo research in the UK. The role of the organisation includes licensing of clinics, setting standards and checking compliance with them through inspections. HFEA also plays a public education role by providing information about treatments and services for the public, people seeking treatment, donor-conceived people and donors.

1.2. Due to the sensitive and confidential nature of the data, it is critical that HFEA operates a robust data recording process, ensuring that for each activity, accurate and timely data is recorded and submitted. The HFEA Register is a large database which holds all the data in one place. Like all large data bases, there are risks associated with maintaining and updating the database.

1.3. HFEA have also established The Information for Quality (IfQ) programme to transform the way data is collected, stored and published.

1.4. During the audit fieldwork we were informed that the programme has closed following:

- The redevelopment of the HFEA website and the Choose a Fertility Clinic search tool;
- The redevelopment of Clinic Portal.

1.5. A new project has been started to deliver the development of an improved system for collecting and reviewing data.

1.6. This review forms part of the HFEA annual audit plan for 2017/2018. In line with the agreed scope, we considered whether:

- A robust approach has been taken to ensure that the high level governance arrangements for the IfQ project are in place, and that all products developed have been subject to expert advice and security testing;
- HFEA have detailed data protection policies, effective guidance, clear reporting processes and robust management checks in place;
- Staff have undergone compulsory annual security training, and that home working arrangements for register team members have been appropriately risk assessed;
- Business Continuity Plans are in place, comprehensive and tested regularly;
- HFEA resource management policies, staff training and contingency arrangements are embedded and reviewed regularly; and
- The controls and processes in place for the data transfer from clinics to HFEA, and how the data register is updated, accessed and reported.

2. Review Conclusion

2.1. The rating for the report is **MODERATE** – some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control. Section Three below provides an overview of the positive assurances we identified as well as areas where we believe improvements can be made.

3. Summary of Findings

3.1. A Chief Information Office role has been created. This will provide HFEA with enhanced strategic stewardship in developing effective strategies and strengthening existing management controls.

3.2. There is a nominated Senior Manager in place with responsibility for day to day information and data management, this provides accountability and facilitates focus on data loss risks and management assurance.

EXECUTIVE SUMMARY

3.3. The newly formed Senior Inspector role should again strengthen oversight of the clinics. We believe that this role should explicitly include oversight over the clinics' information governance and data loss arrangements. This is crucial as it will help clarify HFEA management expectations on the controls registered clinics need to establish over data loss risks and help HFEA discharge its regulatory role. Currently there is limited HFEA management assurance on the governance arrangements clinics have in place to mitigate data loss risks.

3.4. In discussion with HFEA management, we were informed that the IfQ Programme is now closed and this encompassed the delivery of the new website and clinic portal. We have not reviewed the detailed security testing aspects of the new website and clinic portal as a review of the Digital Projects Programme Board minutes demonstrates that the testing had already identified a number of issues. Furthermore, actions and owners had been identified to address these issues and periodic updates were being provided to the programme board on the progress prior to handover as business as usual.

3.5. One of the IfQ programme products was to replace the Register and implement an improved system for collecting and reviewing clinics' data. A separate programme is now underway to complete this requirement - we understand that the details of the programme are yet to be confirmed but in discussion with HFEA management we understand that testing of the security of the system will be built in the process

3.6. There are key detailed polices and processes for both internal staff and registered clinics on how data should be captured and transferred. However, we identified that some of these documents were not up to date or reviewed on a regular basis.

3.7. The HFEA regularly inspects UK fertility clinics and research centres. This ensures that every licensed clinic or centre is adhering to standard safety.The purpose of an inspection is to assess a clinic's compliance with the Human Fertilisation and Embryology Act 1990 (as amended), licence conditions; General Directions and the provisions of the Code of Practice. The results of these audits from 2016/17 have not identified any significant weaknesses. The NAO accopmany one visti per year.

3.8. However, Key policies and some of the Standing Operating Procedures were not up to date and were not reviewed on a regular basis - there is a risk that the policy may be out of date and result in incorrect processes being followed.

3.9. We identified that the HFEA Business Continuity Plan has not been tested on a regular basis. It was therefore not possible for HFEA to provide assurance that the BCP remains current, fit for purpose and reflects key personnel change to ensure roles and responsibilities are clear.

3.10. There was no management assurance documented to demonstrate that all HFEA staff have complete the mandatory e-learning 'responsible for information' training. Therefore, there is a risk that this training has not been carried out by some or all staff resulting in staff handling data incorrectly potentially leading to loss of data;

3.11. The table below summaries the number of recommendations by rating and review area:

	Total Recs	High	Medium	Low
Clinic governance oversight	1	-	1	-
Policy Review	1	-	1	-
Staff Training	1	-	1	-
Business Continuity Testing	1	-	1	-
Overall	4	-	4	-

1.1

4. Next Steps

EXECUTIVE SUMMARY

4.1. To support the provision of a meaningful report to the Audit and Governance Committee you are now required to:

- consider the recommendations made in Section 2; and
- complete section 5 (Recommendations Table: Agreed Action Plan) detailing what action you are intending to take to address the individual recommendations, the owner of the planned actions and the planned implementation date.

4.2. The agreed action plan will then form the basis of subsequent audit activity to verify that the recommendation have been implemented effectively. Management should implement the agreed recommendations before or by the agreed due dates and:

- advise HGIAS that the actions have been completed; and
- provide relevant evidence to demonstrate how the recommendations have been implemented effectively.

4.3. If HGIAS does not receive a response from management by or before the agreed due dates, HGIAS will then follow up all high and medium rated recommendations with the action owner on the relevant due date (as specified in the agreed action plan). This is to verify that the recommendation have been implemented effectively.

4.4. In the absence of a response to our follow up, the outstanding recommendations will be escalated to the relevant Director General and routinely reported to the Audit Committee.

4.5. If management do not accept any of the recommendations made then a clear reason should be provided in the action plan.

4.6. Finally, we would like to thank management for their help and assistance during this review.

5.Recommendations Table

Customer to provide details of planned action; owner and implementation date. Action taken will later be assessed by Health Group Internal Audit, and therefore the level of detail provided needs to be sufficient to allow for the assessment of the adequacy of action taken to implement the recommendation to take place

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE	*EXPECTED EVIDENCE TO DEMONSTRATE RECOMMENDATION IMPLEMENTATION
1.	M	The new Senior Inspector role should include responsibility over the Clinics' governance arrangements in managing data loss, including: a. Clinics' information governance arrangements to mitigate the risk of data losses; b. Clinics' arrangements for staff training on information management; c. Clinics' BCP arrangements.	The Senior Inspector (Information) role has been reviewed and it includes responsibilities for reviewing Information Governance. This includes staff training and security arrangements which includes reviewing BCP planning.	Owner: Chris Hall, Senior Inspector (Information) Inspection regime to be updated to reflect requirements within the new Senior Inspector (Information) post – April 2018	Updated Senior Inspector role document.
2.	M	Key data and information policies should be reviewed periodically to ensure that they are current and aligned.	Information Access Policy and SOPs to be reviewed, updated and ratified to reflect GDPR requirements. Staff Security Procedures (Acceptable Use Policy) to also be updated	Owner: Dan Howard, CIO To align with GDPR legislation and to be updated as a component of the HFEA GDPR Action Plan - May 2018 Update and approve at CMG – January 2018	Updated information policies as outlined in Detailed Finding 2
3.	M	A process should be put in place to ensure that HFEA are able to capture and monitor all mandatory information management learning and development carried out.	We will refresh our approach to the completion of the following modules of mandatory training in IG. Our target is that all	All staff – December 2017. The framework for mandatory training (in all areas including information training requires refresh). In any event whilst many staff	An audit trail demonstrating management oversight of mandatory information management learning and development,

RECOMMENDATIONS TABLE

№	RATING	RECOMMENDATIONS	MANAGEMENT RESPONSE	AGREED ACTION PLAN: OWNER & PLANNED IMPLEMENTATION DATE	*EXPECTED EVIDENCE TO DEMONSTRATE RECOMMENDATION IMPLEMENTATION
			staff will have completed these in the previous 12 months by the end of the calendar year. The modules are: • Responsible for information: general user; • Responsible for information: information asset owner (IAOs to complete); and • Responsible for information: senior information risk owner (SIRO to complete)	have undertaken training within 12 months we will use Oct-Dec period to ensure all staff have completed, with sign off from Managers.	
4.	M	The BCP should be updated on a regular basis to ensure that it reflects all key changes and is appropriately tested to ensure that it is fit for purpose.	BCP test and tabletop test to take place in September 2017. BCP to be updated to reflect lessons learnt from the above tests and to reflect new CIO role responsible.	Owner: Dan Howard, CIO BCP summary test findings report submitted to AGC in October 17. BCP approved by CMG in November 17	Evidence that the BCP is updated and tested regulaly

RECOMMENDATIONS TABLE

1. FINDING/OBSERVATION:

High Level Governance Arrangements: The IfQ Programme has now ceased with the remaining deliverables taken on as a separate project. HFEA have limited management assurance on the clinics governance controls on mitigating data loss.

RISK RATING: MEDIUM

The Information for Quality Programme (IfQ)

To help strengthen and improve data quality and management within HFEA, the IfQ was set up achieve the following:

- The redesign of the website and Choose a Fertility Clinic (CaFC) function;
- The redesign of the 'Clinic portal' (used for interacting with clinics) and combining it with data submission functionality;
- A revised dataset and data dictionary which will be submitted for approval by the Standardisation Committee for Care Information (SCCI);
- A revised Register of treatments, which will include the migration of historical data contained within the existing Register;
- The redesign of HFEA's main internal systems that comprise the Authority's Register and supporting IT processes.

We reviewed the key stakeholders and expert groups consulted on the IfQ programme to ensure that representation was adequate and appropriate. The IfQ Advisory Group comprised of senior stakeholders including expert groups that provided the oversight on subject matter expertise.

We have not reviewed the detailed security testing aspects of the website and clinic portal as a review of the Digital Projects Programme Board minutes demonstrates that the testing had already identified a number of issues. Furthermore, actions and owners had been identified to address these issues and periodic updates were being provided to the programme board on the progress prior to handover as business as usual.

In discussion with HFEA management towards the end of the audit, we were informed that the IfQ Programme is now closed and this encompassed the delivery of the new website and clinic portal. The timeframe for the programme and funding has elapsed for the rest of the deliverables. The Electronic Data Interchange (EDI) replacement system is being taken forward as a separate project and we understand from discussion with HFEA management that new funding has been agreed with the Department of Health (DoH) for this.

Data Governance

The overarching responsibility for HFEA data governance lies with the Director of Compliance and Information. In discussion with HFEA management, we understand that a new Chief Information Officer (CIO) is being recruited. This is a key role ensuring that there is senior leadership and stewardship of information management from a strategic perspective. The findings below are

interrelated and the role of the CIO will be crucial in bringing a strengthened approach to data management.

In addition, during the audit we were informed that a new Senior Inspector (Information) post is being created to strengthen information governance and provide assurance and a challenge function to the clinics regarding information management responsibilities. The purpose of this role is to focus on licensed centres' performance relating to their information responsibilities. The Senior Inspector is yet to be confirmed, but the position will be in place for autumn. This will provide a much needed oversight for the clinics. To further strengthen information governance, we believe that HFEA should ensure that Senior Inspector role explicitly covers the clinics' governance arrangements on how data loss risks are managed.

RISK/IMPLICATION:

Without appropriate management assurances over clinics governance arrangements, there is a risk that clinics may implement ineffective governance arrangements which may result in the materialisation of data loss risk and consequent reputational damage to HFEA.

RECOMMENDATIONS:

1. The new Senior Inspector role should include responsibility over the Clinics' governance arrangements in managing data loss, including:
    a. Clinics' information governance arrangements to mitigate the risk of data losses;
    b. Clinics' arrangements for staff training on information management;
    c. Clinics' BCP arrangements.

2. FINDING/OBSERVATION:
The key policies are in place but they need to be periodically reviewed to ensure that are aligned with processes.

RISK RATING: MEDIUM

There are a number of data/information policies within HFEA. This includes:

- The HFEA's Information Access Policy, with a number of Standing Operation Procedures (SOPs). The policy sets out the general principles that will be adopted by the HFEA in response to any requests for information under any statutory access regimes, with particular reference to recording and monitoring requests for information. The policy is easily accessible via the intranet system (last reviewed 2011).

- Staff Security Procedures - this policy sets out guidelines on acceptable use of IT resources and information security within the HFEA (last reviewed 2015).

- Information Access SOPs - these documents set out how HFEA will ensure effective processing of requests for information, openness and transparency of the HFEA as a public body; consistency of response and process; proper delegation of responsibility to subject

experts; and cultural change in the HFEA's management of enquiries and its fulfilment of its statutory role as an information provider (last reviewed 2012).

These are key Policies and therefore the HFEA management team should ensure that they are reviewed periodically to ensure that the policies and processes are aligned. The issue of updating policies has previously been raised twice in the 16/17 HFEA audit on Request for Information IT and the 14/15 report on FOIs and PQs.

A draft version of updated Information Access policy was provided. Although the policy is currently under review, there is no reference to the new the General Data Protection Regulation (GDPR) which comes into effect in May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR and therefore it is crucial that HFEA are compliant with the updated regulations. There is a 2017/18 internal audit planned on GDPR, and so we will not be raising a recommendation on this issue in this report.

There are a number of general guidance documents available for clinics to adhere to when collecting and recording information. These are easily accessible via the clinics new portal.

RISK/IMPLICATION:
Without periodic review of key polices there is a risk that staff may follow incorrect processes leading to data loss and reputational damage.
RECOMMENDATIONS:
2. Key data and information policies should be reviewed periodically to ensure that they are current and aligned.

3. FINDING/OBSERVATION: **Management do not have assurances in place to confirm that all staff members have completed the mandatory annual information management e-learning module.**
RISK RATING: MEDIUM

Staff Training

HFEA have a Learning and Development policy in place. The aim of this policy is to ensure that all HFEA employees are aware of the procedures for applying for a learning opportunity, to ensure that all CPD requirements are met and that all employees have equal access to learning and development opportunities. This policy places responsibility on the line manager to ensure that their staff members complete the mandatory training. There a number of training requirements that the policy classifies as mandatory, the most significant for this audit is the 'responsible for information' training. In discussion with HFEA management, it is not clear how management have obtained assurance that all HFEA staff completed this important training.

Homeworking

HFEA facilitates homeworking for its staff. Previously a risk assessment form was required to be carried out to ensure that appropriate security protocols were in place for those staff members that handle personal information at home. However, this requirement was superseded by a working at

home policy that was issued in 2011 but not reviewed since. Whilst the details in the policy are adequate, the policy should be reviewed to ensure that it is current and aligns to best practice and that the line manager and staff agree working at home protocols. A recommendation covering review of key polices has been covered in the above section.

Clinics' Training

In addition, it is not clear on what training clinic staff have available to them in respect of information management. From discussions with management, we understand that each clinic will have autonomy to set standards that comply with the general requirements stipulated by the Information Commissioners Office (ICO). However, given that the HFEA is UK Government's independent regulator overseeing fertility treatment and research, we think that it is important that HFEA has a level of oversight/assurance on clinics' training programmes regarding information handling. A recommendation covering assurance over clinics' information management training has been covered in the above section.

RISK/IMPLICATION:

Without assurance that staff members have undertaken the appropriate information training, there is a risk that staff may handle data incorrectly leading to the loss of data and resulting in reputational damage.

RECOMMENDATIONS:

3. A process should be put in place to ensure that HFEA are able to capture and monitor all mandatory information management learning and development carried out.

4. FINDING/OBSERVATION:
The Business Continuity Plan needs to be updated to reflect the changes in the organisation and tested to ensure that it is fit for purpose.

RISK RATING: MEDIUM

Business Continuity Planning (BCP)

The Director of Finance & Resources is responsible for ensuring business continuity arrangements are in place. The BCP states HFEA has made a business impact assessment and that no areas of operation would be critical for at least seven days. After that time, it may be critical to issue licences or special directions, or suspend a licence. In addition, at certain times, some activities would be judged critical, such as confirming payroll or attending to legal issues.

This document is owned by the Head of IT, who is responsible for reviewing this plan on a regular basis, ensuring that the document is kept up to date, that up to date copies of the document are held by key staff and that the plan is tested. However, we noted that the Head of IT has left the organisation and this has not been updated on the plan.

A review of management minutes demonstrates that the BCP was tested as regards staff communication protocols. This was carried out in 2016. A BCP test has not been conducted to gauge the effectiveness of the actual BCP. HFEA should undertake, at minimum, a desktop

exercise periodically to identify any issues with the current BCP arrangements and implement any lessons learnt. In discussion with management regarding the BCP arrangement that clinics have in place, it was established that currently there is no BCP oversight from HFEA over the clinics. The new Senior Inspector role provides an opportunity for HFEA to build in some management assurance over clinic BCP arrangements.
RISK/IMPLICATION:
Without appropriate BCP testing there is a risk that the BCP may not be fit for purpose and delay the recovery of key processes resulting in reputational damage.
RECOMMENDATIONS:
4. The BCP should be updated on a regular basis to ensure that it reflects all key changes and is appropriately tested to ensure that it is fit for purpose.

5. FINDING/OBSERVATION: **There is no specific resource management policy, but it is a standing discussion topic in the senior management team meeting.**
RISK RATING: LOW
There is no specific resource management policy, as a small organisation the Corporate Management Group (comprising SMT and Heads) is responsible for oversight of the workforce and resourcing. There is a standing item 'resources and prioritisation' which ensures that every area of the organisation can be involved in that discussion and/or raise issues. The resources and prioritisation' minutes demonstrate discussion regarding ongoing vacancies, HR frameworks, PDPs, capacity of teams. A learning and development policy has been developed and is available on the intranet - the aim of the policy is to ensure that all HFEA employees are aware of the procedures for applying for a learning opportunity, to ensure that all CPD requirements are met and that all employees have equal access to learning and development opportunities. No concerns were raised in the Corporate Management Group minutes we reviewed relating to the resourcing of information governance.

6. FINDING/OBSERVATION: **Data is submitted via a portal that is only accessible by licensed clinics through standard templates; a new project is underway to replace the register that holds clinical data.**
RISK RATING: LOW
Licensed fertility clinics submit information about each cycle of treatment they carry out, such as patient and donor details, the treatment provided and its outcome. This information is held on a database called the Register. The requirement to keep a Register of Treatments stems from the Human Fertilisation and Embryology Act 1990 (as amended) (the Act). The Register is an extremely valuable asset to HFEA and its stakeholders. It is used to: • Securely hold information about donors and their donations;

- ensure traceability of gametes and embryos;
- provide patient information on success rates;
- monitor clinic performance; and
- facilitate research into the safety of treatments.

The Register is held on a spreadsheet on an internal server and is known as the EDI. One of the IfQ programme products was to replace the EDI and implement an improved system for collecting and reviewing data, as discussed earlier in the report. A separate programme is now underway to complete this requirement, we understand that the details of the programme are yet to be confirmed but in discussion with HFEA management we understand that testing of the security of the system will be built in the process. The Register Information Manager, she has confirmed that access to the register is restricted. It is limited to her team, one IT lead, Director Of Compliance & Information and the Interim Head of Information.

The HFEA website contains a clinic portal to which clinics submit their information. Clinics are expected to manage their own access control and data management from their side. Data is sent by clinics via the portal into the EDI system. There are number of set forms available on the HFEA intranet with associate guidance on what forms to use for specific actions.

Annual audits are undertaken at clinics by the inspectorate team as part of the licence renewal inspection with the NAO accompanying one audit per year. The purpose of an inspection is to assess a clinic's compliance with the Human Fertilisation and Embryology Act 1990 (as amended), licence conditions; General Directions and the provisions of the Code of Practice. Inspection reports are prepared by the inspection team and are publicly available on the HFEA website. In discussion with HFEA management we understand that informal feedback is directly provided to the person responsible at the centre. We were unable to obtain the NAO report for 2016/17, however in the published HFEA Audit and Governance Committee meeting, the NAO reported that the interim audit at the HFEA had just been completed and that there were no significant issues identified. The NAO would be visiting a clinic based in Cambridge in April 17 as this is part of the external audit process.

Suggested Risk Ratings:

Priority	Description
HIGH	Fundamental weaknesses in control which expose the Accounting Officer / Director to high risk or significant loss or exposure in terms of failure to achieve key objectives, impropriety or fraud. Senior managers are expected to oversee the prompt implementation of agreed actions, or to confirm in writing that they accept the risks of not implementing a high priority internal audit recommendation.
MEDIUM	Significant weaknesses in control, which, although not fundamental, expose the Accounting Officer / Director to a risk of loss, exposure or poor value for money. Managers are expected to oversee the prompt implementation of agreed actions, or to confirm in writing that they accept the risks of not implementing a medium priority internal audit recommendation. Failure to implement recommendations to mitigate these risks could result in the risk moving to the High category.
LOW	Minor weakness in control which expose the Accounting Officer / Director to relatively low risk of loss or exposure. However, there is the opportunity to improve the control environment by complying with best practice. Suggestions made if adopted would mitigate the low level risks identified.

Report Rating – Definitions

Substantial	In Internal Audit's opinion, the framework of governance, risk management and control is adequate and effective.
Moderate	In Internal Audit's opinion, some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	In Internal Audit's opinion, there are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.

RECOMMENDATIONS TABLE

Unsatisfactory	In Internal Audit's opinion, there are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.