INFORMATION SECURITY ARRANGEMENTS WITHIN THE CARE QUALITY COMMISSION

EXTERNAL REVIEW REPORT

FOR THE CHIEF EXECUTIVE OF THE CARE QUALITY COMMISSION

31 AUGUST 2016

CONTENTS Page

This review was conducted by Chris Hurran with the helpful assistance of a number of members of CQC.

Executive Summary

The aim of this review was to investigate the loss of 4 lever arch files containing Disclosure and Barring Service (DBS) certificates which was reported internally in CQC on 11 July 2016 and occurred in the margins of CQC office refurbishment works in Newcastle on 8/9 July. The review was required to establish relevant facts and causative factors with regard to the data loss incident, to review the incident response, to examine relevant information security policies and procedures and to make recommendations.

The review was carried out by interviewing CQC staff, inspecting CQC premises, reviewing CQC documentation, and by open source research.

The review agrees with the conclusion of an earlier internal CQC Serious Incident Report that the missing documents are unlikely ever to be recovered, that CQC are unlikely ever to establish their final disposal and that theft was unlikely. The review is confident that there was no malicious intent on the part of any CQC staff in the data loss. The missing documents were held in accordance with CQC retention policy and as Protection Rating 5 documents their loss represents a very serious data loss incident.

The main organisational enabling factors which led to the data loss included the failure to recognise information risk in the office refurbishment project when it should have been self-evident in an information business such as CQC, non-compliance with CQC's own information security policy and failure to follow and manage the project plan.

The review concluded that neither the prime contractor nor the sub-contractor responsible for furniture removal can be held responsible for the data loss (although failings of both contributed to it).

The review found that the overall information security architecture of CQC is fundamentally sound. The review believes, however, that there is a mismatch between the expectations of CQC Information Security Policy and the actual behaviours of some CQC staff. Whilst many may be highly compliant, there is clear evidence that this is not universal and a culture shift is needed to change this. This incident should provide CQC with the impetus to make the organisation-wide culture change that is needed in order to be the exemplary information security organisation it aspires to be against the background of "Safe Data, Safe Care".

The review makes 6 recommendations. Two of these relate to information risk management and one to incident response management and all are easy to implement. Two relate to supply chain risk management and, whilst they merit early attention, they may take longer to implement. The final recommendation is the most important but also the most challenging and relates to the need for organisation-wide culture change to equip CQC for an exemplary role in a "Safe Data, Safe Care" society.

Introduction, Purpose and Terms of Reference

On 11 July 2016 a serious data loss was reported internally in CQC. The loss took place in the margins of CQC office refurbishment works in Newcastle on 8/9 July and concerned 4 lever arch files containing Disclosure and Barring Service (DBS) certificates.

This external review was carried out in August 2016 on the instructions of the Chief Executive of CQC. CQC's objectives were to establish relevant facts and causative factors with regard to the 8/9 July data loss incident, to review the incident response, to examine relevant information security policies and procedures and to make recommendations. The full terms of reference are attached at Annex A.

Methodology

Information to meet the requirement was obtained by:

- Open source research (including publicly available references listed at Annex D),
- Reviewing internal CQC documentation (including those references listed at Annex D),
- Inspecting CQC premises at Citygate, Newcastle,
- Interviewing CQC staff (face to face and/or telephone). Those interviewed are listed at Annex B.

The Information Commissioner's Office (ICO), the Department of Health (DoH) and the DBS Authority were not consulted and their responses to the data loss incident, if any, do not form part of the review.

The prime contractor and the furniture removal sub-contractor were not interviewed. It was thought that their evidence would add little to understanding of the data loss incident and, although they clearly played a role in events, they bear no responsibility for the related information risk.

The Data Loss Incident that Prompted this Review

The review was informed by the Serious Incident Report[(1)] which is attached at Annex C for convenience. This information was supplemented through interviews of CQC staff. The Serious Incident Report is comprehensive and largely accurate and therefore not repeated in detail here. However, the following points are drawn out either to improve accuracy or for reasons of emphasis:

- For many reasons (but including the transparent attention to procedural detail of the CQC DBS team and their energetic, but in the event futile, response to the loss) the review is confident that the 4 missing lever arch files were indeed present in the cabinet in question (referred to hereafter as "the DBS cabinet") when the DBS team locked up on Friday 8 July.
- The 4 missing lever arch files contained 418 DBS certificates and 77 DBS reprints, a total of 495 missing documents. The applicants identified in the reprints did not contain DBS 'information' however they still contained the applicant's address and job description.
- In addition to the 4 missing lever arch files and some blank and letter headed stationery, a number of other items present in the DBS cabinet on lock up on 8 July were found to be missing on 11 July. These included a box file with Return to Sender mail (which CQC had attempted to return on more than 3 occasions without success), post received on 8 July

(which included one disclosure (with shows) and 2 reprints) and the recorded delivery post book.

- The DBS cabinet itself was not present anywhere in the Citygate building on 11 July, including not in the under croft (where some office furniture was still awaiting eventual removal). Nor were the 4 missing lever arch files in any of the numerous black rubbish bags in the under croft or anywhere else on CQC's Citygate premises.
- Neither the DBS cabinet nor the 4 missing lever arch files were subsequently found during searches of other sites.
- The "limited amount of paperwork" found during searches of black bags on 15 July (described in the Serious Incident Report) included sensitive documents which probably came from the Inspection Team (3rd Floor, East Wing, Citygate building). One of these documents was a notice of proposal to refuse to a provider and another was internal documentation relating to administrative arrangements for a hospital inspection. As these documents were recovered, there was no loss and no harm. However, the fact that these documents left CQC premises in rubbish as part of the removal process suggests that CQC can have no certainty that other sensitive documents might not also have been removed in a similar manner. But, as any such documents were not found during the searches, the probability is that they have now been disposed of and will never be recovered. (See also below on the Office Improvements Project.)
- The DBS certificates contained in the 4 missing lever arch files were being correctly held within CQC document retention policy. Although not listed on the Information Asset Register (see also below on Information Security), they would have been categorised as Protection Rating 5 ("High volumes of identifiable confidential personal data or of sensitive and potentially reidentifiable personal data" and "Not publically available, very high sensitivity, high likelihood of very significant impact on key relationships, high likelihood of very significant reputational harm to CQC")

The review drew the following conclusions about the incident itself:

- The review agrees with the conclusion of the Serious Incident Report that the 4 missing lever arch files (or any of the other missing items) are unlikely ever to be recovered and that CQC is unlikely ever to establish their final disposal.
- The review is confident that there was no malicious intent on the part of any CQC staff in the data loss.
- The review agrees with the conclusion of the Serious Incident Report that theft of the missing files is unlikely. With the passage of time since the data loss, the possibility of theft reduces still further. Even if the documents were stolen it is hard to see how a thief could exploit them other than by trying to embarrass CQC.
- The missing documents were held in accordance with CQC retention policy and as Protection Rating 5 documents their loss represents a very serious data loss incident.

The CQC Newcastle Office Improvements Project – Organisational Enabling Factors that Led to the Data Loss

In addition to the information obtained from CQC staff interviews and that contained in the Serious Incident Report, the review was informed about the CQC Newcastle Office Improvements Project (referred to hereafter as "the project") from the following sources:

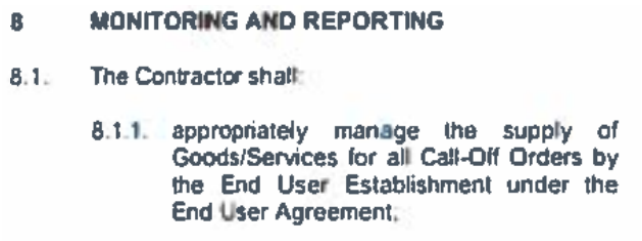
- Design Build Services ITT Part A Final dated 9 September 2015[2]
- A redacted version (commercial details removed) of the ESPO Framework Agreement between CQC and the prime contractor dated 19 November 2015[3] (referred to hereafter as "the contract")
- Notes from the Project Board meeting of 29 April 2016 dated 3 May 2016[4]
- Newcastle Office Improvements Bulletin dated May 2016[5]
- Daily Plan of Works (for Phases 2, 2a, 3 3a and 4 of the project) dated 22 June 2016[6]
- Office Improvements Risk Report dated 11 February 2016[7]
- Citygate Project Status Report dated 11 February 2016[8] (and other project status reports which added no additional useful information and which are therefore not referenced)

Information Risk:

Nowhere in any of the documentation (in particular the Risk Report referenced above) was there any mention of information risk or wider security considerations. The fact that information risk was not considered during the project planning or management was confirmed through CQC staff interviews. Its omission is recognised in hindsight as having been an error. (Comment: CQC is an information business. Potentially there is some level of information risk in even the most trivial activity (eg a member of staff leaving their computer unlocked when they go to make a cup of tea and additionally being overheard gossiping about sensitive work at the tea point). In particular, there is always information risk in office moves, furniture replacement or renovation projects. Mitigating procedures to reduce the risk should always be considered as part of the project plan of all projects which are subject to formal project management.)

CQC relationship with the prime contractor and furniture removal sub-contractor:

The contract with the prime contractor follows a standard format with no special modifications for this project. The following extracts from the contract are of relevance to the data loss incident:



8 MONITORING AND REPORTING

8.1. The Contractor shall:

8.1.1. appropriately manage the supply of Goods/Services for all Call-Off Orders by the End User Establishment under the End User Agreement.

9 CONTRACTOR'S PERSONNEL

9.1. The Contractor shall select, employ, train, furnish and deploy in and about the performance of the End User Agreement only such persons as are of good character and who are appropriately skilled and experienced.

9.2. The Contractor and the Contractor's sub-contractors, staff and agents shall comply with all reasonable requirements of the End User Establishment.

9.3. The Contractor shall use reasonable endeavours to ensure that its sub-contractors are subject to the provisions of clauses 9.1 and 9.2 above.

9.4. The Contractor, its agents, sub-contractors and suppliers shall employ sufficient staff to ensure that the Goods/Services are supplied at all times, including periods such as staff holidays, absence through sickness or any other cause.

General Requirements

1. Take account of any CQC estate strategy, estates design principles, Financial Business Case models, or alternative strategy or direction provided within a specific brief;
2. Provide risk management solutions that minimise disruption to the business;
3. Provide robust plans to manage any implications for DDA and Health and Safety requirements of staff during and after the move;
4. Upon completion of projects to produce buildings management documents, for example, floor plans, electrical drawings, operation and maintenance manuals and; documents associated with buildings statutory testing, for example, and electrical and other testing certificates, water risk assessments, and any Asbestos register;
5. Take full account of current legislation, Government Guidance and Best Practice (including but not limited to Achieving Excellence, Revitalising Health and Safety, Sustainable Development, Sustainable Operations on the Government Estate, Design Quality, Gateway Reviews);
6. Ensure that any advice provided complies with CQC values and business objectives;
7. Prior to or upon receipt of every order to undertake services, provide an initial report setting out their detailed understanding of the brief, proposed approach to the task, resource plan and fee proposal, and must agree the level of expertise and experience of the personnel to be involved with the Client;
8. Where Project Management and Full Design Team services result in any changes to the CQC estate, the supplier is to provide all necessary assistance and information to update the CQC property records;
9. Provide and maintain personnel with appropriate qualifications and experience in the relevant professional disciplines and specialist areas;
10. Provide and maintain personnel with adequate knowledge of health and safety legislation and good practice, environmental and security issues which are relevant to the projects covered by the framework;
11. Ensure that the services, projects and programmes of work are progressed and delivered within the agreed fees and approvals;
12. Ensure that the services, projects and programmes of work are progressed and delivered within the required timescales;
13. Ensure that the work complies with the specification and meets appropriate professional, technical, quality, safety and environmental standards and current Government education and social care standards and guidelines;
14. Ensure that the work complies with Contracting Authorities' policies and procedures;
15. Demonstrate the ability to effectively review service delivery in order to continually improve performance;
16. Demonstrate the commitment to help raise standards

Interviews confirmed that there were no additional instructions given by CQC to the prime contractor in writing with regard to any aspect of security. The prime contractor's staff were not briefed on CQC Information Security Policy. The prime contractor was ultimately responsible for the furniture removal part of the project sub-contracted to the furniture removal sub-contractor.

Neither the prime contractor employees nor the furniture removal sub-contractor employees involved in the contract were subject to any security clearance. (Comment: All CQC staff have as a minimum BPS clearance.)

Various references in the contract to the appropriate handling of confidential information are considered irrelevant to the circumstances of the data loss because neither the prime contractor employees nor the furniture removal sub-contractor employees could have been expected to know that they were handling such information.

In summary, in delivering the project the prime contractor was responsible for providing appropriately qualified staff of good character both from themselves and from the furniture removal sub-contractor; they were responsible for monitoring the activities of the furniture removal sub-contractor; and they were expected to comply with CQC policies and procedures (but could only do so with those of which they were aware). There were no additional expectations with regard to security or information risk management.

The agreed removal procedure for locked furniture:

The Serious Incident Report highlights the agreed procedure in the event that the removals team encountered locked cabinets marked for removal ("any cabinets which were marked for removal or needed moving and found to be locked should be forced open and the contents left in the CQC office".) This procedure was agreed verbally between CQC and the prime contractor and it is presumed that the latter briefed the furniture removal sub-contractor accordingly. Whilst in hindsight this procedure is obviously flawed and is the fundamental cause of the data loss, there is some background which explains why such an inappropriate procedure should ever have been contemplated. An interviewee explained that during an earlier move from Finsbury Tower, CQC staff totally failed to clear cabinets as instructed, causing significant problems to the office move. Despite the entreaties to Newcastle CQC staff (eg in the May bulletin referenced above), there was a management expectation that there could be problems (with locked cabinets marked for removal) for the furniture removal sub-contractor team which might potentially derail the project. It is now recognised in hindsight that a different procedure should have been used (eg CQC staff certifying empty all cabinets planned for removal).

Local management and modifications to the project plan:

The Serious Incident Report describes in detail the modifications to the project plan which were agreed orally between a number of members of CQC staff and a representative of the prime contractor on 6 and 7 July. The review noted that the local CQC project manager was on leave during the week of the data loss and that the overall CQC project manager was in London.

The review agrees with the conclusion of the Serious Incident Report that the lack of adherence to the documented plan and a misunderstanding between CQC staff and the prime contractor team was a significant cause of the data loss.

CQC supervision on 8 and 9 July:

Para 8.1.1 of the Information Security and Governance Policy (ISGP)[17] (see below) states:

Areas that hold, store and/or process personal data are automatically classed as secure areas. Only authorised persons are permitted access to these areas, visitors must be escorted at all times. Computer screens and documents in use in such secure areas are to be protected at all times from being viewed by unauthorised persons.

The review noted that at an earlier stage of the overall project (in Leeds), CQC staff had initially supervised furniture removal until this was cancelled on cost savings grounds. No CQC staff supervised the work at Citygate on 8 or 9 July. The review also noted, with approval, that following the data loss incident subsequent project work at Citygate was supervised by CQC staff.

The decision not to have CQC supervision of the furniture removal was in breach of CQC's own policies and was a significant contributory cause of the data loss.

The activities of the prime contractor and the furniture removal sub-contractor at Citygate on 8 and 9 July:

The review did not interview the prime contractor or the furniture removal sub-contractor staff and so the events that took place in CQC's Citygate offices on 8 and 9 July can only be deduced from secondary sources. Two points are worthy of note:

- We know from the building manager's contractor pass records that a representative of the prime contractor was present on 8 July but **not** on 9 July. On 9 July, therefore, the furniture removal sub-contractor staff were totally unsupervised. Arguably this is a breach of the contractual relationship (referenced above) between CQC and the prime contractor but this is not considered material to the data loss. However, greater engagement from the prime contractor might have contributed to incident response and building a better picture of what had happened.
- We know (again from the building managers) that the security doors for the 3rd and 4th floors were found (on the morning of Monday 11 July) still to be wedged open. This had clearly been done by the furniture removal sub-contractor team to facilitate furniture removal without having to repeatedly swipe in and out. This reflects badly on the building managers as it proves that they failed to comply with daily lock down procedures after the the furniture removal sub-contractor team left Citygate on 9 July. Theoretically this could mean that other persons unknown could have accessed CQC premises between 9 and 11 July and removed the 4 missing lever arch files. However, this is considered unlikely. It does mean however that access records for the 4th floor will not provide useful evidence. This might have been important (see below on Incident Response) in identifying exactly who might have removed the cabinet and/or the 4 missing lever arch files.

The review concludes that CQC organisational enabling factors that contributed to the data loss were:

- The significant failing that CQC did not recognise that there was information risk in the project.
- The failure to certify furniture as being empty before removal contributed to the risk of an information security incident.

- The failure to supervise external contractors was in breach of CQC's own policies and removed a safety mechanism that might have prevented the data loss.
- The project governance did not control locally agreed late modifications to the project plan and the resultant confusion directly led to the data loss.

The review further concludes that neither the prime contractor nor the furniture removal sub-contractor can be held responsible for the data loss (although failings of both contributed to it).

The review makes one recommendation in this respect:

Recommendation 1: CQC should consider information risk to be by default an integral element of all projects which are subject to formal project management. If a decision is made by the SRO that the circumstances of a particular project makes information risk irrelevant then that decision should always be documented and endorsed by the SIRO.

Incident Response following the Data Loss

The review was informed by the Serious Incident Report and by CQC Information Security Incident Management Procedure (ISIMP) dated 26 September 2012[9] but noted that a new Crisis Management Plan (not seen) was in the late stages of approval.

An important element of incident response (and noted in Para 5 "Managing the Incident" of ISIMP) is to establish and maintain a document log recording all the documents produced and gathered as part of the investigation and to maintain a chronological audit log of all events and evidence supporting decisions taken during the incident. Neither of these were done and this made it difficult for the review to establish the exact timeline of the incident and who was in charge and when. The CQC Information Security Manager was not informed until 1600 on Monday 11 July. It was clear, however, that a number of things were done well:

- The timely and comprehensive searching of CQC Citygate offices and under croft.
- The subsequent searches of the furniture removal sub-contractor sites on 14 and 15 July.
- The high quality of record keeping by the DBS team that enabled detailed identification of what was missing.
- The prompt reporting to the ICO, DoH and DBS Authority.
- The individual letters sent to all those members of the public affected (copy attached at Annex E).
- The decision to make a public statement.

The review formed the opinion that there was only a growing awareness of the severity of the incident and hence the need for decisive action, especially in the early stages. One interviewee described it as a "creeping crisis" and another said that "decisions were made on the hoof, reactively and jointly". The Crisis Management Team (CMT) was never formally stood up. In the light of this it is not surprising that opportunities may have been missed:

- It is not clear that firm instructions were passed to the prime contractor (and through them to the furniture removal sub-contractor) at the earliest possible opportunity to freeze all

disposal activity with regard to the removed furniture and rubbish. The Serious Incident Report refers to "These discussions established that approximately half of the furniture removed from Citygate had already by destroyed or broken up for scrap or recycling." The review is surprised that the furniture removal sub-contractor had completed so much processing so quickly and before its disposal could be halted on CQC instructions.

- An early attempt was made to find out if the CCTV (particularly in the under croft) revealed anything of value but the CCTV coverage was not seen by CQC staff. The building managers said that they could not provide this access to CQC staff but that they would review it themselves. When the review requested this coverage, the building managers said that it was only retained for 30 days and therefore no longer available. No attempt was made by CQC to obtain the access records to CQC premises on 8 and 9 July. We now know that, because the doors were wedged open, these records would in fact not have provided useful information. (Comment: Contracts with third party suppliers should always include the ability to obtain audit information in real time for the purpose of managing incidents or investigating wrong doing. This is particularly important with regard to suppliers of IT services and building management services but there will be others as well.)

The review concludes that:

- Despite the absence of record keeping and the fact that the CMT was never stood up, CQC's response to the incident was actually very effective. This reflects well on the energy, initiative and commitment of all involved.
- Although some opportunities to acquire evidence or recover documents may have been missed they do not add significantly to the seriousness of the incident or CQC's ability to resolve it.

The review makes two recommendations in this respect:

Recommendation 2: Existing contracts with third party suppliers should be reviewed to ensure that they provide for the provision of audit information in real time for the purpose of managing incidents or investigating wrong doing. Future contracts should include this provision by default.

Recommendation 3: Once the new Crisis Management Plan has been formally approved it should be exercised (perhaps with a complex data loss incident scenario involving electronic data).

<u>CQC Information Security - From Board Strategy to Workplace Practice</u>

The review took a snapshot of information security arrangements from board level strategy through corporate policy to working practices within teams. In July 2016 CQC published its Policy Statement on Information Security and Governance[(10)] which, in the wake of the "Safe Data, Safe Care" security review[(11)], includes a section on how CQC's own data is secured and used. The review took this statement as the baseline for judging CQC's actual information security performance.

Information security is appropriately recognised on CQC's Strategic and Operational Risk Register[(12)] as Risk OR8:

CQC Strategic and Operational Risk Register 2016-17

	Oversight /Owner	Description of Risk 2016-17	Pre Impact	rating Likeli hood	Rating	Controls and mitigations * *Specific actions continue to be refined and embedded into business plans during Q1.	Current Impact	Rating Likeli hood	Rating	Confid ence in ability to manage
High level Operational risks (and Business plan priorities)										
Priority 3 – Build an effective; efficient; learning and values based CQC										
OR8	ACGC Exec Dirs CCS S&I	Risk that we are not protecting or securely managing our **information** effectively in accordance with regulatory requirements, agreed standards and legislation	4 - High	3 - Medium	12 - Medium	**Controls** - Information management and governance policies, Induction and awareness training, Access and security controls, Senior Information Risk Owner supported by the Information Governance Group (IGG), Internal audit programme **Mitigating actions** · Completion of annual information governance assessment · Audits to test effectiveness of ICT controls	4 - High	3 - Medium	12 - Medium	High

The Executive Director of Strategy and Intelligence is also the Senior Information Risk Owner (SIRO). It is not clear how ownership of this risk is shared between the SIRO and the Executive Director of Customer and Corporate Services. By chance, the current SIRO assumed his interim appointment on 11 July 2016 (the date the DBS data loss was identified), following the departure of his predecessor the previous week. There is no suggestion that any lack of clarity as to the ownership of Risk OR8 might have contributed to the DBS data loss incident or the subsequent response. Although the review makes no recommendations in this respect, CQC may wish to consider whether shared risk ownership is beneficial in managing this risk (see also below).

The review noted that the Audit and Corporate Governance Committee (ACGC) provides effective oversight of Risk OR8. The ACGC recognises that "It is important that (CQC) continues to be an exemplar in this area" (ie information security and governance)[13]. In addition to the regular review of all risks at its quarterly meetings (which includes reviewing the register of information security incidents), the ACGC gave detailed consideration to information security risk at its meetings on 3 February 2016[13] and 31 March 2015[14]. In addition to the register of information security incidents, the ACGC monitors CQC performance on the annual NHS Information Governance Toolkit return. The review observed that the IG Toolkit returns show consistent and commendable improvement over the last 4 years:

	2015-2016		**2014-2015**		**2013-2014**		**2012-2013**	
	Overall Score	**Reviewed Grade**	**Overall Score**	**Reviewed Grade**	**Overall Score**	**Reviewed Grade**	**Overall Score**	**Reviewed Grade**
Information Governance Management	86	Satisfactory	86	Satisfactory	86	Satisfactory	73	Not Satisfactory
Confidentiality and Data Protection Assurance	88	Satisfactory	76	Satisfactory	76	Satisfactory	61	Not Satisfactory
Information Security Assurance	90	Satisfactory	90	Satisfactory	86	Satisfactory	75	Not Satisfactory
Overall	89	Satisfactory	85	Satisfactory	84	Satisfactory	69	Not Satisfactory

The second tier of information security risk management is provided by the Information Governance Group (IGG) which is chaired by the SIRO. The IGG maintains a comprehensive risk register[15] which appears to capture all relevant information security risks (but see also below). The risk most relevant to the DBS data loss is Risk 25:

Information Risk Register

Title:	Information Risk	Project Lead:	Simon Richardson	Updated on:	26-May-16
		Project Sponsor:	Malte Gerhold	Updated by:	Information Governance Group

Ref	Risk Reference No.	Risk Description	Impact of Risk on Objectives	IGG Risk Owner	Mitigating Action and Controls (Current)	Mitigating Action and Controls (Planned)	Action Owner	Current Risk level after action			Effectiveness of Mitigation/ Latest Commentary	Date risk last reviewed
								Impact (5 - Very High; 4 - High; 3 - Medium; 2 - Low; 1 - Very Low)	Likelihood (5 - Very High; 4 - High; 3 - Medium; 2 - Low; 1 - Very Low)	Risk Rating (V High, High, Medium, Low)		
25	CONFIDENTIALITY R06	CQC information is lost or inappropriately accessed due to unauthorised person(s) gaining access to CQC property or offices	Reputational damage. Loss of public trust. Unwillingness of whistleblowers and public to disclose information to CQC. Enforcement action/fine from ICO.	Derek Wilkinson	Access controls (locked doors, security passes, CCTV, security and reception staff) in place in all CQC offices. Password controls on computers, locked storage and clear desk policy minimise the information accessible to any intruder.	Protective Security checks of CQC offices being carried out Out of hours security reviews of CQC office space carried out with regular ongoing reviews	Derek Wilkinson	3 - Medium	1 - Very Low	3 - Low		04-Feb-14

The risk description is accurate and the impact is correctly stated. It was at least partly due to failings in the current mitigating actions and controls that the data loss occurred. The review addresses wider aspects of some of these points further below but notes that Risk 25 should be expanded to include authorised, non-CQC persons who might exploit their legitimate access for unauthorised purposes and include as a mitigating action that non-CQC persons with authorised access should normally be supervised by CQC staff. It should be noted that this is in accordance with Para 8.1.1 of the Information Security and Governance Policy (ISGP)[17] (see below)

Recommendation 4: The IGG risk register Risk 25 mitigating actions should be expanded to include the normal requirement for non-CQC visitors to CQC premises to be appropriately supervised.

The IGG is also the body which ratifies the ISGP. The review saw two versions of this. The published version is that dated 24 October 2012[16] for which the name of the responsible committee/individual is listed as the IGG. The more recent unpublished version is dated 31 October 2015[17] for which the name of the responsible committee/individual is listed as the Executive Director of Customer and Corporate Services. This raises again the issue addressed above about the ownership of Risk OR8. It would be normal for a SIRO to be responsible for an organisation's Information Security and Governance Policy.

The review focussed on the 31 October 2015 version of the ISGP. The review noted that the policy is intended to apply to all CQC business areas and 3rd party suppliers. It is therefore the policy that should have guided the relationship between CQC and the prime contractor over the Newcastle Office Improvements Project when it came to matters of information security.

The ISGP makes frequent reference to the fact that it is supposed to apply throughout the CQC supply chain:

The Security Policy applies to all premises, physical equipment, software and data owned or managed by CQC, directly or indirectly through sub-contractors, to deliver services. This scope particularly includes the data relating to authorised CQC users and providers that is stored or processed. Depending on the source of the data, CQC is both a 'data processor' and 'controller' according to the definitions within the *Data Protection Act 1998*.

Some computing facilities, such as the end-user client desktops with third party contractors, are outside the direct management control of CQC. However, where they are used to process CQC data they still fall within the scope of this Security Policy. The security requirements are included within the relevant contract with the contractor.

Further detail is provided at Para 9.2 of ISGP. The review noted, however, that the IGG risk register makes no reference at all to information security risks in the CQC supply chain. The single reference to a supplier is made in Risk 10 which lists "Audit checks to be conducted using IT logs provided by Atos" as a mitigating action and control. It may be that the IGG, in applying its own ISGP, assumes that the term "CQC" in its risk register is intended to be interpreted as "CQC and all its sub-contractors and third party contractors". However, even if this is the case, the review believes that lack of specific reference to supply chain information security risk makes it all too likely that potentially serious mistakes could occur. A new risk should be added to the IGG risk register which addresses generic supply chain information security risk and, as mitigation, allocates appropriate accountability to CQC staff to ensure that the contractual arrangements do indeed address information security risks and that those contractual arrangements are subject to appropriate audit. Such a risk of course applies most importantly to CQC IT suppliers but the Newcastle Office Improvements Project shows that it also has relevance more widely. There is an implication in the CQC Policy Statement on Information Security and Governance[(10)] that this is being done already but the relevant actions need to be enshrined in the governance framework through the risk register.

Recommendation 5: The IGG risk register should have an additional risk fully addressing information security risks in the CQC supply chain.

In all other respects the ISGP comprehensively covers all the subjects expected in an information security policy. In particular, there are no obvious gaps or weaknesses with regard to the expected behaviours of CQC staff and their line managers. Potential high risk areas such as remote working are covered effectively. It was not part of the review's remit to check compliance with the latter but CQC will want to satisfy itself that the culture and compliance issues referred to below also apply to remote workers.

In common with the security policy of many organisations, the ISGP places an obligation on all CQC staff to comply with the policies and a copy of the ISGP is available to all staff on the CQC intranet. However, the ISGP combines required working practices for all employees (including the less IT literate) with specialist policies for systems administrators etc. It is not reasonable to expect all CQC employees to read all 98 pages of the ISGP in order to be conversant with every policy applicable to them. CQC goes some way to address this challenge by the use of the Information Security Quick Guide[(18)]. Whilst this document should be familiar to all CQC readers of this review, a copy is attached at Annex F for convenience. In addition, CQC mandates annual information governance and security training and a regular supply of awareness training materials are made available to staff. Further comments on the effectiveness of these arrangements are made below.

Alongside the IGG in the second tier of information security risk management (and subordinate to the SIRO) are the nominated Information Asset Owners (IAOs) and Information Asset Administrators (IAAs). The review examined the Information Asset Register (IAR)[19]. The latest version was approved by the IGG and published on 2 June 2016. The review made no attempt to audit the IAR but noted that it appeared to be fully in accordance with good practice – the exemplar which CQC seeks to be in information security risk management. The section of the IAR dealing with the DBS records is:

IAR Series	Asset number	Asset Title	Asset Description	Format	Business Area/owner	Security/ protective marking	Protection Rating	Vital record	Retention	Retention notes	In public domain
014. Registration records	14.5	Disclosure and Barring DBS-successful		Electronic	Registration (ASC Directorate)	Yes	5	No	6 months after final registration decision/notice of decision		No
014. Registration records	14.6	Disclosure and Barring-unsuccessful		Electronic	Registration (ASC Directorate)	Yes	5	No	6 months after final decision - (including appeals, tribunal etc.)		No

Series	Information Asset Owner	Information Asset Manager	Business area
014. Registration records	(Adrian Hughes), Sally Warren,	Julia Denham	Registration - North & Central
		Deborah Cotton-Soares	Registration - South

The review noted that this latest version of the IAR has clearly been drafted in a forward looking way. Thus there is actually no reference to the hard copy DBS records which were of course those which went missing. The hard copy records are in the process of being phased out and replaced by the new electronic format. Although theoretically this is an error, the review is of the opinion that it would have made no difference to the data loss incident had the hard copy records been listed alongside the electronic ones. Accordingly the review makes no recommendations in this respect. It should also be noted that data retention of the hard copy DBS records which went missing was in accordance with the old policy (12 months) which was being diligently applied.

Beneath these tiers of information security and governance described above lie the actual working practices of CQC staff. The review did not have the remit or capacity to properly survey CQC staff information security behaviour and compliance but some observations were made during 3 visits to CQC premises (2 to Buckingham Palace Road (BPR) and one to Citygate, Newcastle) and through relevant information obtained from interviewees (baselined against the Information Security Quick Guide[18]):

- Passes: A small but significant number of staff do not visibly wear their passes. Some CQC staff were observed still wearing their passes in the street in BPR. Tailgating at the main door and internal doors of BPR is common, including by staff not wearing passes. One interviewee said that there are very occasional instances of pass sharing at Citygate.
- Training: Most interviewed staff were asked if they had completed their annual training and all who were asked claimed that they had. This was supported by an interviewee who confirmed that the majority of staff do their training.
- Clear desks: An early morning visit to Citygate showed the review that there is good compliance with the clear desk policy on the 3rd and 4th floors. However, one interviewee commented that a significant number of staff were non-compliant with locking their

computer screens when they are away from their desks during the working day and the review also noted instances of this occurring at Citygate.

- Retention, Disposal and Destruction: The management expectation of non-compliance with regard to disposal (described above) and the discovery of sensitive papers in black bags at the furniture removal sub-contractor site on 15 March are indicative that there is a problem here.

The review believes that there is a mismatch between the expectations of CQC Information Security Policy and the actual behaviours of some CQC staff. Whilst many may be highly compliant, there is clear evidence that this is not universal and a culture shift is needed to change this. Tolerance by an organisation's management of non-compliance with policy undermines the effectiveness of policy generally and gives employees implicit licence to pick and choose which policies they will comply with and which they will ignore. It also undermines staff with security and/or risk management responsibilities. The imperative for CQC to be an exemplar organisation against the background of "Safe Data, Safe Care", combined with the wakeup call of this data loss incident, means that this is an ideal time for CQC to embark on a programme of culture change across the organisation, from top to bottom. There are many ways of approaching this but the review commends to CQC's consideration some of the relevant CPNI products (eg the Workplace Behaviours Campaign[20] and the security culture tool SeCuRE[21]).

Recommendation 6: CQC should embark on a programme of security culture change so that they can become an exemplary information security organisation in the context of "Safe Data, Safe Care".

Conclusions and Recommendations

The loss of DBS certificates as part of an office refurbishment project in CQC's Newcastle offices was a very serious but entirely avoidable incident. The organisational enabling factors which caused it included the failure to recognise information risk in the project when it should have been self-evident in an information business such as CQC, non-compliance with CQC's own information security policy and failure to follow and manage the project plan. But there was no malicious intent and there is much evidence that the incident response (albeit with some failings of process) was good and that the overall information security architecture of CQC is fundamentally sound. There is, however, something of a mismatch between policy and compliance. This incident should provide CQC with the impetus to make the organisation-wide culture change that is needed in order to be the exemplary information security organisation it aspires to be against the background of "Safe Data, Safe Care".

The review makes 6 recommendations summarised below:

Recommendation 1: CQC should consider information risk to be by default an integral element of all projects which are subject to formal project management. If a decision is made by the SRO that the circumstances of a particular project makes information risk irrelevant then that decision should always be documented and endorsed by the SIRO.

Recommendation 2: Existing contracts with third party suppliers should be reviewed to ensure that they provide for the provision of audit information in real time for the purpose of managing incidents or investigating wrong doing. Future contracts should include this provision by default.

Recommendation 3: Once the new Crisis Management Plan has been formally approved it should be exercised (perhaps with a complex data loss incident scenario involving electronic data).

Recommendation 4: The IGG risk register Risk 25 mitigating actions should be expanded to include the normal requirement for non-CQC visitors to CQC premises to be appropriately supervised.

Recommendation 5: The IGG risk register should have an additional risk fully addressing information security risks in the CQC supply chain.

Recommendation 6: CQC should embark on a programme of security culture change so that they can become an exemplary information security organisation in the context of "Safe Data, Safe Care".

Annex A

Review Terms of Reference

Terms of Reference for the external review of information security arrangements within CQC.

Background

Following a serious data security loss reported internally on 11th July 2016, the Chief Executive has requested that an independent, external review of the circumstances of the data loss, and CQC's response is carried out.

External reporting of the details of this incident has been completed, along with an initial internal investigation of the incident, and a commitment to commissioning this independent review.

Incident Summary

A major programme of works to refurbish CQC offices in Newcastle and Leeds were carried out between 31st May and 24th July. One phase of the refit to the office in Newcastle was carried out on 8th and 9th July. During that phase 4 lever arch files were lost, these files contained sensitive Disclosure and Barring Service (DBS) information relating to 500 individuals.

Description of the review

The review is intended to focus on circumstances surrounding the data loss, but in so doing, to be able to provide findings and recommendations which are applicable to the wider organisational context.

The following elements should therefore be delivered within the scope of this review:

- An investigation into the circumstances of the data loss itself, which builds on the internal investigation already carried out, intended to establish so far as possible, the relevant facts, and causative factors. So far as is relevant, this should include consideration of any applicable CQC policies and procedures.
- Consideration of CQC's response to the incident, in particular relevant risk and incident management practice, and those governance arrangements relevant to the response.
- In order to enable organisational learning, in respect of the matters covered by the review, identification of any areas of CQC practice that are either well managed or would benefit from review or change.
- The production of a report, which will be published, that addresses the issues outlined above and makes recommendations.

The Commission will:

- Provide a contact person with whom an external investigator can liaise and who can provide necessary assistance.

- Ensure that the Investigating Officer is provided with all necessary information to allow them to complete their investigation.
- Provide names and contact details of all parties identified as being part of the investigation.
- Ensure that those people in the direct employ of the Commission are available for interview as part of the investigation and are appropriately aware of the nature and scope of the enquiry.

Timescales:

The commencement date of this investigation is the 1 August 2016. The Investigating Officer should aim to complete his investigation and deliver a report to the Chief Executive on the areas identified by 31 August 2016. Should it become apparent that there is good reason to extend this timescale, the Investigating Officer should communicate this to the Director of Governance and Legal Services.

Signed: ……. Date:…5/8/16……..

Annex B

CQC Staff Interviewed by the Review

Julie Craig

Andrew Evans

Sarah Edwardson

Malte Gerhold

Kate Harrison

Martin Harrison

Caroline Nixon

Paul Oliver

Martin Pitcher

James Schubeler

Derek Wilkinson

Annex C

Serious Incident Report

Loss of Disclosure and Barring Service (DBS) Certificates

25th July 2016

Introduction

On Monday 11th July 2016 4 lever arch files containing up to 500 copies of disclosure certificates were found to be missing from the Citygate offices. The cabinet which had been used to store copies of the DBS certificates, in 6 lever arch files, had been removed from the office along with redundant furniture as part of a planned office refurbishment.

The planned office refurbishment works in Citygate took place in a number of phases between 31st May and 24th July. Phase 3a of these works took place between the 6th and 9th July and covered the removal of cabinets on the 3rd floor of the building. However, that work also encompassed late changes to the project plan including last minute alterations on the 4th floor which was where the DBS certificate cabinet was located.

The DBS certificates which have been lost contain personally identifiable data including any details of criminal convictions, including spent convictions.

Background

As part of the CQC Newcastle and Leeds office refurbishment programme, arrangements were made with a project management company (Primary Contractor) to competitively tender on behalf of CQC for office refit and removal services. These contracts were awarded to selected sub-contractors for the removals and refit services. The removal services covered the removal and disposal of redundant furniture.

Project plans were produced covering all of the intended refit arrangements for both offices, the plans were broken down into 4 phases between 31st May and 24th July with some minor out of hours phases (2a and 3a). Those plans included diagrams of the offices annotated with the existing and planned layout as well as indicating the furniture to be disposed of.

Phase 3a of the project was planned for Friday 8th July from 17:00 to 22:00 but overran and was completed between 8:00 and 12:00 on Saturday 9th July.

Members of the primary contractor staff, CQC facilities and NCSC staff discussed the phase 3a works on site on Wednesday 6th July, cabinets on both the 3rd and 4th floors were then clearly labelled with 'Remove' stickers by a member of the primary contractor staff. Phase 3a of the project originally only covered furniture on the 3rd floor but was extended to elements of the 4th floor to provide additional storage and improve the aesthetics of the office space.

Further discussions took place on 7th July on the 3rd floor where it was decided to revert to the original plan and retain some of the cabinets marked for removal the previous day. Labels on the cabinets on that floor were changed to reflect this new requirement. However, the labelling on the 4th floor cabinets was not amended as it was understood by the primary contractor that the late change of plan related to the 3rd floor only. This resulted in the cabinets on the 4th floor remaining labelled for removal.

At 16:45 on 8th July members of the DBS team locked the files containing the DBS certificates away in accordance with their end of day procedures and secured the key to the cabinet in the key safe. They have stated that they did not notice any sticker on the cabinet indicating that it had been identified for removal.

This phase of the work was subsequently carried out by the sub-contractor staff during the evening of the 8th July and the morning of the 9th July. Access to the offices had been arranged with the building security team and they were accompanied by project management staff from the primary contractor. There were no CQC staff on site when this work was carried out.

There was an agreement between CQC, the project management company and the removals service that any cabinets which were marked for removal or needed moving and found to be locked should be forced open and the contents left in the CQC office. When the DBS team returned to work on Monday 11th July they found their cabinet missing with 2 of the 6 lever arch files containing copies of DBS certificates on top of another, nearby cabinet. A book of royal mail stickers used by the team which had been stored in the cabinet was also found nearby. The other 4 files, containing the copies of the DBS certificates, could not be located.

The missing files contained copies of DBS certificates dating from July 2015 to March 2016. An electronic system was introduced on 1st April 2016 meaning that no certificates were copied and stored as hard copy since that date. The copies of the certificates were being stored for up to 12 months, in compliance with the records retention policy.

Comprehensive searches of the Citygate offices and outside storage and rubbish areas were carried out on 11th July but did not locate the files. All confidential waste

bins were opened and checked by CQC staff. Those searches did not find the missing files.

Urgent discussions took place with the 2 companies involved in the move to establish the whereabouts of the cabinet. These discussions established that approximately half of the furniture removed from Citygate had already by destroyed or broken up for scrap or recycling. The remaining items were being held in storage at a sub-contractor facility, that site was searched by CQC and contractor staff on the 14th and 15th July. Those searches also failed to recover the lost documentation.

The company has informed CQC that any documentation found during the dismantling process would have been removed from the furniture, stored and would be returned by courier to Citygate. A limited amount of paperwork has been returned to CQC as well as other documentation found during the searches on the 15th July. None of that documentation relates to the DBS files or individual certificates.

Throughout all phases of the project staff were informed that they must remove all documentation and other items from their storage cabinets and store them in temporary blue crates which could be sealed. This was done as the removals company would not be able to move very heavy full cabinets. The DBS team had moved from the 3rd to the 4th floor on 20th June and had already relocated all of their documentation from its previous storage cabinet on the 3rd floor to their new area and re-allocated storage cabinet on the 4th floor. They have stated that they understood that their involvement in the move was complete and no longer had to empty any cabinets they were using. It was from the cabinet on the 4th floor that the files were lost as it had been included in the last minute changes which the team was unaware of.

Checks carried out by the DBS team have established that the 4 lost files contained copies of DBS certificates relating to 500 individuals. The team has produced a comprehensive list of those individuals along with their contact details.

This incident was reported to the Information Commissioner's Office (ICO), the Department of Health and the DBS authority on 15th July 2016. The ICO has acknowledged the report and indicated that they will follow up in due course.

Conclusions

It is concluded that:

- The root cause of the loss of these documents was the last minute verbal changes to the requirements for the contractors made on 7th of July, the lack of adherence to the documented plan and a misunderstanding between CQC staff and the primary contractor team.

- The last minute changes to the project plan were not subject to any change control or approved by the project board.

- The project widely communicated details of the project and the requirement to secure documentation in scope of the project to all staff in the Newcastle and Leeds offices.

- Contractor staff were given access to CQC offices with no on-site presence of CQC staff.

- Contractors were given instructions to remove all furniture marked for removal, if they found furniture which contained any items then they told to force open the item and leave any contents in the office.

- This incident represents a very serious data security breach potentially causing harm or distress to 500 individual members of provider staff.

- Despite comprehensive searches both internally and externally, the missing files cannot be located.

- Should the information contained in the missing folders fall into unscrupulous hands then is has the potential to cause further harm and distress to the individual data subjects.

- Whilst theft of the files cannot be ruled out at this stage, it is believed to be a very low likelihood.

- It is believed likely that these files will never be recovered and we will not be able to establish their final disposal.

Recommendations

It is recommended that:

- CQC should inform each of the subjects of this data breach in writing.

- CQC should assist any further investigation by the Information Commissioner's Office in their subsequent follow up on this incident.

- Details of this incident should be published on the CQC website to provide a summary of the breach.

- An internal communication should be made to all staff on the intranet to provide an overview of the incident. Teams which may be involved in follow up to the incident

should be provided with a more detailed report, this includes the engagement, information access, legal and complaints teams.

- All future office moves and refurbishment should be subject to comprehensive management oversight including security team review of the plan and appropriate input.

- All future access to CQC offices by contractor staff should be directly overseen and supervised by CQC staff.

- All projects should include comprehensive change control procedures with clear approval paths to project boards.

- Consideration should be given to commissioning an independent, external review of CQC security arrangements.

Investigating Officer:

Information Security Manager – CQC

25th July 2016

Annex D

References:

1. CQC Serious Incident Report dated 25 July 2016, Available at: https://www.cqc.org.uk/sites/default/files/20160727_report_loss_of_DBS_certificates.pdf (Accessed 26 August 2016)
2. Design Build Services ITT Part A Final dated 9 September 2015
3. Redacted version (commercial details removed) of the ESPO Framework Agreement between CQC and The prime contractorGroup Ltd dated 19 November 2015
4. Notes from the Project Board meeting of 29 April 2016 dated 3 May 2016
5. Newcastle Office Improvements Bulletin dated May 2016
6. Daily Plan of Works (for Phases 2, 2a, 3 3a and 4 of the project) dated 22 June 2016
7. Office Improvements Risk Report dated 11 February 2016
8. Citygate Project Status Report dated 11 February 2016
9. CQC Information Security Incident Management Procedure dated 26 September 2012
10. CQC Policy Statement on Information Security and Governance, July 2016, Available at: http://www.cqc.org.uk/sites/default/files/20160411%20Final%20Policy%20Statement%20on%20Information%20Security%20July.pdf (Accessed 22 August 2016)
11. "Safe Data, Safe Care" CQC report into how data is safely and securely managed in the NHS, July 2016, Available at: http://www.cqc.org.uk/sites/default/files/20160701%20Data%20security%20review%20FINAL%20for%20web.pdf (Accessed 22 August 2016)
12. CQC Strategic and Operational Risk Register 2016-17, Available at: https://www.cqc.org.uk/sites/default/files/201600623_strategic_operational_risk_register_201617.pdf (Accessed 22 August 2016)
13. CQC ACGC Paper No ACG/02/16/04 dated 3 February 2016.
14. CQC ACGC Paper No ACG/03/15/27 dated 31 March 2015.
15. CQC IGG Information Risk Register dated 26 May 2016.
16. CQC Information Security and Governance Policy dated 24 October 2012, Available at: https://www.cqc.org.uk/sites/default/files/documents/20121115_information_security__governance_policy.pdf (Accessed 22 August 2016).
17. CQC Information Security and Governance Policy dated 31 October 2015.
18. CQC Information Security Quick Guide, undated, Available at: http://www.cqc.org.uk/sites/default/files/CQC%20Information%20Security%20-%20quick%20guide.pdf (Accessed 22 August 2016).
19. CQC Information Asset Register dated 2 June 2016.
20. CPNI Workplace Behaviours Campaign, Available at: http://www.cpni.gov.uk/advice/Personnel-security1/Workplace-behaviour-campaign/ (Accessed 29 August 2016)
21. CPNI Security Culture Tool SeCuRE, Available at: http://www.cpni.gov.uk/advice/Personnel-security1/Security-culture/ (Accessed 29 August 2016)

Annex E

CQC

Citygate

Gallowgate

Newcastle upon Tyne

NE1 4PA

Telephone: 03000 616161
Fax: 03000 616171
www.cqc.org.uk

<Date>

Dear [insert name]

Loss of disclosure and barring service (DBS) certificates

I am writing to inform you about an incident which has occurred at our CQC office in Newcastle. It has resulted in the loss of 500 copies of disclosure and barring service (DBS) certificates. Based on our records we believe this includes a copy of your DBS certificate.

I am clear that this very serious mistake should never have happened. I can only apologise for the loss of your record, as well as for any distress or concern it may cause you, which I deeply regret. We have undertaken a thorough internal investigation to understand why this information has been lost and to ensure a similar loss will not occur in the future.

I have also asked for an independent external review of our actions which will be reported to the CQC Board when completed. We have also reported the incident to the Information Commissioner's Office who will be conducting an independent investigation and publishing a summary report on their findings.

The incident occurred on Saturday 9 July 2016 during a planned refurbishment of our Newcastle office. It appears that the locked filing cabinet containing the DBS documentation had been wrongly marked for removal and destruction. Once the loss was identified, a thorough and comprehensive search of the CQC offices and of the storage company's facilities owned by the removal company was carried out. Unfortunately, this has not resulted in the documents being located or recovered and we believe them to be irretrievably lost.

CQC retains a copy of all DBS certificates which reference a criminal conviction or are required for reference purposes for a period of 12 months after the application has been approved. The

certificates which have been lost relate to the period from July 2015 to March 2016. A new online system was introduced on 1 April 2016 which has removed the need for paper copies to be retained.

I will write to you again following the outcome of the report from the Information Commissioner's Office and if any significant information on this incident comes to light.

If you have any questions or concerns regarding the information in this letter please contact our National Customer Service Centre on 03000 616161 or at enquiries@cqc.org.uk

Once again, please accept my sincere apologies for this incident and for any concern it may cause you. A copy of this letter has been sent to all individuals we believe to be affected.

Yours sincerely

David Behan

Chief Executive

Annex F

Care Quality Commission

QUICK GUIDE

Information Security

This leaflet defines information security and governance and provides summarised advice from the CQC Information Security and Governance Policy document. It has been produced as a quick reference guide and contains the top ten good practice pointers to assist staff in their day to day business activities.

Information is an asset within CQC which, like other important assets, has value to our business activities and consequently needs to be appropriately protected.

Information security measures are designed to protect information from a wide range of threats in order to ensure that our information is appropriately secure, accurate and available when we need it. This can be summarised as:

Confidentiality	Ensuring only those who ought to have access can do so
Integrity	Ensuring that information cannot be modified without detection
Availability	Ensuring that information can be accessed when needed

Information can exist in many forms. It can be printed, handwritten, stored electronically or as digital images. The information may be transmitted by post or electronically.

Information security is achieved by implementing a suitable suite of controls, which include policies, practices, procedures, organisational structures and software/technical controls.

Some aspects of information security and governance are contained within legislation. The most notable UK Acts are:

- **Data Protection Act**
- **Computer Misuse Act**
- **Freedom of Information Act**
- **Public Records Act**

Additionally, staff are under a common law obligation to preserve the confidentiality of service user information.

Information security will only be successful with the active participation of all staff.

More detailed information can be found on the intranet - see **Directorates and Teams > Governance & Legal Services > Information Security**

Good Practice 'Top 10'

Passwords

Ensure that you change your passwords regularly (the applications will prompt you) and use strong passwords with at least 8 characters and a combination of at least 3 of the following; lower case, upper case, numbers and special characters.

Passes

Wear your CQC pass visibly in our offices and ensure that you take them off when you leave the building. Do not let people tailgate you into our access controlled areas and challenge anyone who tries to do so.

Training

Completion of IG and Security training is an annual requirement mandated by the Cabinet Office. Please take the time to complete the training package on the Marton House website as soon as possible during each financial year.

Homeworking and Travel

The same security measures apply when you are working at home or on the move to those required in the office. Additionally, CQC assets, both electronic and hard copy, should be safeguarded when in transit and whilst in your home environment.

Email and Encryption

Personal and sensitive information should not be contained within the body of emails being sent outside of the CQC trusted network. If you do need to send this kind of information outside CQC ensure that it is encrypted within an attachment.

Social Media

Social media is a useful communications tool used increasingly by CQC. Unauthorised personal use of social media should not contain CQC information whether considered sensitive or not.

Unsolicited Communications

It is common to receive emails and calls from unknown sources or sales representatives. These may also include attempts to get you to reveal corporate or personal information (phishing). If you receive such communications do not reply - simply delete the email and report the matter to the security mailbox. However, if you think the request may be a legitimate request for information, please forward it to information.access@cqc.org.uk immediately.

Clear Desks

All documents containing personal and sensitive information should be locked away outside normal business hours. Computers should be shut down at the end of the working day and have the screen lock applied (Ctr, Alt & Del, then hit 'Enter') if you are going away from your desk for lunch or a meeting.

Retention, Disposal and Destruction

Retention periods for data in CQC has been defined in the schedule published on the intranet by the Knowledge and Information Management team. Once data is no longer required it should be destroyed securely in line with CQC Information Security and Governance Policy available on the intranet.

Incident Reporting

In the event that something does go wrong, or you suspect that there may have been a data breach, please report it to the security mailbox: security@cqc.org.uk

If you have any questions about anything in this leaflet or the wider Information Security Policy and Procedures, please contact security@cqc.org.uk or the Information Security Manager (Derek.wilkinson@cqc.org.uk) directly.