Review Of FOI Request 12/131 – Prof. Ross Anderson

(Review completed on 10/08/2012)

1. Purpose Of Internal Review

The purpose of this internal review is to determine whether the MHRA dealt properly with the applicant's request under the Freedom of Information Act (FOIA)

The terms of reference of this review are:

- To read all correspondence between the applicant and the Agency, and other relevant correspondence;
- To form an opinion on the handling of the correspondence by the Agency;
- To advise whether the actions taken by the Agency in reaching their decisions is justified under the FOIA;
- To make recommendations for further action by the Agency if appropriate; and
- To prepare a report of the review for the Agency and the requester.

2. Introduction

The initial request from Prof. Anderson was made on 17/03/12 (annex A), and was answered by MHRA on 18/04/12 (annex B).

Prof. Anderson was not satisfied with the reply and requested an internal review of the Agency's decision on 04/05/12 (annex C).

The Agency attempted to resolve the situation informally on 22/06/12 (annex D), seeking some clarification as to exactly what information was required, and providing some additional information on the form of a report previously withheld.

Prof. Anderson remained dissatisfied in his reply dated 05/07/12 (Annex E) and a formal internal review then became necessary

3. Background

Prof Anderson wrote in on 17/03/12 with a number of questions relating to the Agency's Clinical Practice Research Datalink (*CPRD). These questions had to do with issues around security, anonymisation, risk assessments etc.

The Agency replied on 18/04/12, dealing with each question in turn either providing the requested information, refusing and citing an exemption, or seeking further clarification where the questions appeared unclear.

As he was dissatisfied with the reply he wrote in on 04/05/12 requesting an internal review of the Agency's decision. This request focused on the non disclosure of a paper ("Privacy protection and research access mechanisms for National Health Service Data: The Clinical Practice Research Datalink") which contained much of the information Prof. Anderson was seeking in his original request (although this paper was not specifically mentioned in that request), the Agency's application of the S43 exemption, and further observations regarding the Agency's position regarding security mechanisms.

The Agency replied to this on 22/06/12, on an informal basis, to see if a resolution could be found short of a formal internal review. This reply listed items where clarification was still needed, items that it was believed the Agency had answered, and items that had been withheld

under Section 43. Prof Anderson was invited to clarify the outstanding issues and confirm that he had had a satisfactory reply to several others. This reply also expanded upon and clarified the Agency's use of Section 43 which appeared to have been misapplied in the original answer (this is covered in sections 4 & 5 below). The paper previously referred to was also provided as there were no applicable exemptions.

Prof. Anderson remained dissatisfied and wrote in again on 05/07/12. This reply did not directly address the points raised in the Agency's reply of 22/06/12, but –in addition to providing some interesting historical background and commentary on system security- did boil down what the Agency believed he still required that he felt had not been provided:

"documentation you assembled (including meetings of minutes you held) to assess what the threat would be to your system, and the top-level strategy you adopted in order to manage the resulting risks"

"details of how the security policy was implemented by means of inference control mechanisms, audit procedures and other protections"

As this information is still considered non-disclosable a formal internal review has been undertaken

* CPRD is the NHS observational and interventional research service, building on the work undertaken by the MHRA's General Practice Research Database (GPRD) Division. The General Practice Research Database has been operating since 1987, and has been managed by the MHRA (and its predecessor body, the MCA) since 1999. Throughout that time, anonymised data has been collected from General Practices throughout the UK and made available for health benefiting research.

4. Consideration Of The Issues

Use of exemptions

The Agency's initial reply on 18/04/12 cited Section 43 (commercial interests) and then implied that this section had been applied to preserve the security of various systems. This is, of course, incorrect.

Section 43 states:

"**43.** - …(2) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice the commercial interests of any person (including the public authority holding it)."

There is nothing in the exemption to cover any issues relating to security. The Agency's informal communication of 22/06/12 acknowledged this error, and went on to confirm that Section 43 applied, and outline the commercial impact that would, or would be likely to, result from disclosure.

Although there is nothing in Section 43 relating to security issues, the data maintained by CPRD is commercially valuable as it is supplied to researchers for a fee.

CPRD has a market pricing structure for access to the data and services. Service costs are priced based upon time of staff and use of specific IT systems. Data costs are charged at a fixed rate depending upon which data sources are required and the complexity of linkage. Therefore, any disclosure that is likely to prejudice this operation falls clearly within the scope of Section 43.

The potential consequences of disclosure are basically twofold:

- Any disclosure under the FOIA is effectively a disclosure to everyone, it would give malicious attackers information which may assist them in compromising the systems. This could corrupt or make data unavailable to fee paying researchers, and it would be reputationally damaging if it could be demonstrated that CPRD systems were not secure.

- Secondly, disclosure could allow competitors to benefit from the considerable –and costly- developmental work that has gone into the creation and maintenance of CPRDs systems. Avoiding the necessity to fund such work would allow a competitor to undercut on fees.

Prof. Anderson's arguments in favour of disclosure

Much of Prof. Anderson's argument in favour of disclosure seems predicated on the suggestion that if CPRD have in place adequate measures to ensure security, there would be no harm in disclosing information that proves the robustness of the systems (this would be Auguste Kerckhoffs principle that a system should be secure even if everything about it, except the key, is public knowledge). He also specifically mentions in his emails "security-by-obscurity" (i.e. a system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that if the flaws are not known, then attackers will be unlikely to find them).

On its own, a system relying upon "security-by-obscurity" would, of course, be inadequate, and the suggestion that the MHRA is relying on "security through obscurity" in its original response, is not correct. The MHRA takes a "defense in depth" approach to its IT security, which is not "obscured" but is subject to annual independent technical review and risk assessment by a Communications-Electronics Security Group (CESG) Check accredited organisation. However, there are more recent views, following Kerchkoffs' work (which dates back to 1883 and relates to cryptography), that in a defense in depth approach to IT systems, some elements of obscurity have a valid place.

Furthermore, there is a definite difference between subjecting systems to independent review and making the entirety of the IT systems security a matter of public availability. Shannon's maxim states that "the enemy knows the system", it does not state that one should provide it to them.

5. Conclusion and recommendations

In the Agency's initial reply dated 18/04/12, Section 43 was cited. However, the accompanying justification for its application was misleading in that it implied that the exemption was related to system security rather than commercial prejudice. Prof. Anderson correctly identified this error and raised it in his internal review request

The answering Division were aware that their argument was based on commercial prejudice, and that the prejudice would arise from a breach of security. They were made aware of the lack of clarity in their reply, and the issue was clarified in the informal reply of 22/06/12. The Agency apologises for any confusion caused to Prof. Anderson.

Moving on the actual application of the exemption, it is of course important, and in the public interest, that systems containing data –especially of a sensitive nature- are secure, and can be shown to be secure by means of relevant independent testing and audit (a process MHRA undergoes annually, as such testing is required and mandated by the Cabinet Office).

This does not mean however, that it is necessarily sensible or in the public interest to disclose detailed information that may serve to compromise that security.

As stated in the Agency's reply of 22/06/12, failure of the business model arising from disclosure of information following a request under the Act would prejudice research activity benefitting the public health which derives from it. Added to likely commercial prejudice the Agency believes that the public interest remains clearly weighted in favour of maintaining the exemption.

Therefore, the Agency's view that Section 43 is engaged in respect of this information stands.

On a final note, it might provide some measure of reassurance to Prof. Anderson to know that the MHRA's Director of Information Management and Senior Information Risk Owner (SIRO), Alison Davis -although now a civil servant- has over 25 years of IT experience, gained predominantly in the pharmaceutical and chemical industries, before joining the Agency in 2006.

If Prof. Anderson remains dissatisfied, he may ask the Information Commissioner (ICO) to make a decision on whether or not we have interpreted the FOIA correctly in dealing with the request and subsequent internal review. The ICO address is listed below:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Mr S Wilson - FOI Officer, MHRA Policy Division

Annex A

-----Original Message-----
From: Ross Anderson [mailto:request-109883-2ea71462@whatdotheyknow.com]
Sent: 17 March 2012 13:47
To: MHRA Central Enquiry Point
Subject: FOI 12/131 - Freedom of Information request - Privacy mechanisms in CPRD

Dear Medicines and Healthcare products Regulatory Agency,

Please supply me with all the information you have about the privacy design for the Clinical Practice Research Datalink (CPRD) including

- the threat model;
- the security policy;
- any assessments submitted to or performed by third parties including the ICO and CESG;
- design documents for the privacy enhancing technologies in use or contemplated;
- the design documents and evaluation reports for any trusted third party used for data linkage;
- contracts with operators of trusted third parties and policy documents specifying the protocols to be used for record linkage, service level agreements, liability and audit requirements;
- full details of how encryption will be used as a privacy enhancing technology;
- full details of any other linkage or anonymisation methods used when longitudonal records are assembled from data contributed by different healthcare providers;
- any assessments that have been performed of other potentially personally identifying information released to researchers in addition to encrypted patient and practice identifiers;
- full details of statistical security and inference control mechanisms used to assess and control queries submitted interactively to CPRD by researchers;
- full details of the query audit mechanisms that will be used to detect abuse of non-interactive access after the fact;
- any technical assessments of the combined effectiveness of query auditing plus data perturbation, of the effect of data perturbation on the clinical dependability of perturbed data, and of any design trade-offs made between privacy and clinical dependability;
- copies of the agreements that CPRD users will have to sign to get access;
- copies of any legal opinions sought by the MHRA on the legality of CPRD and in particular its compliance with DPA 1998 and with S8 ECHR;
- any privacy impact assessments performed for CPRD.

Yours faithfully,

Ross Anderson
http://www.ross-anderson.com

Annex B

By email to

Ross Anderson

request-109883-2ea71462@whatdotheyknow.com

Ref No: FOI 12/131
18 April 2012

Dear Professor Anderson

Thank you for your email of 17 March 2012 in which you requested information about Privacy Mechanisms in CPRD. We have now completed searching for the information you requested.

A copy of the information, which can be disclosed, is enclosed.

The remainder of the information that you requested is exempt under section 43 of the Freedom of Information Act. I have explained at each stage in the attached document the reasons for the exemption.

If you are dissatisfied with the handling of your request, you have the right to ask for an internal review. Internal review requests should be submitted within two months of the date of receipt of the response to your original letter and should be addressed to: Policy Division FOI Unit, MHRA, 151 Buckingham Palace Road, London SW1W 9SZ. Please remember to quote the reference number above in any future communications. If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Yours sincerely,

Dr John Parkinson
CPRD Director
John.parkinson@mhra.gsi.gov.uk

To set the context for our reply, I'd like to provide a little background. The CPRD was launched on 29 March 2012 as the new NHS observational and interventional research service. However, it builds substantially on the work undertaken by the GPRD Division of the MHRA. The General Practice Research Database has been operating since 1987, and has been managed by the MHRA (and its predecessor body, the MCA) since 1999. Throughout that time, anonymised data has been collected from General Practices throughout the UK and made available for health benefiting research. You can view the bibliography of research publications at http://www.cprd.com/Bibliography/

Please supply me with all the information you have about the privacy design for the Clinical Practice Research Datalink (CPRD) including

- the threat model;

We treat what we consider threats in a whole series of ways but to enable us to answer your request we will need to understand what you mean by this request. If you are able to explain what it is you are asking for we will endeavour to provide the information.

- the security policy;

It is not clear to us what you mean by this request. If you are able to explain what it is you are asking for we will endeavour to provide the information.

- any assessments submitted to or performed by third parties including the ICO and CESG;

We have sought and will continue to seek assessments of the security of our systems. However, the nature of such assessments detail the security provisions we have in place, and their disclosure may provide external parties with intelligence to assist them in attacking our system security. This could give rise to risk to our operations, and in turn the public-health benefiting research undertaken using our services. We would therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by maintaining the highest levels of security, which will enable the research undertaken using our data and service to continue.

- design documents for the privacy enhancing technologies in use or contemplated;

We use various privacy enhancing technologies to ensure that information we hold is secure. However, the nature of such technologies is such that their disclosure may provide external parties with intelligence to assist them in attacking our system security. This could give rise to risk to our operations, and in turn the public-health benefiting research undertaken using our services. We would therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by maintaining the highest levels of security, which will enable the research undertaken using our data and service to continue.

- the design documents and evaluation reports for any trusted third party used for data linkage;

See below

- contracts with operators of trusted third parties and policy documents specifying the protocols to be used for record linkage, service level agreements, liability and audit requirements;

The design documents and contracts for the provision of trusted third party services contain information about the provision of such services which if disclosed could be used by other organisations to gain an advantage, for reasons of commercial gain. We therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by preserving our ability to provide services which are to the benefit of public health.

- full details of how encryption will be used as a privacy enhancing technology;

We use various encryption techniques to ensure that information we hold is secure. However, the nature of such technologies is such that their disclosure may provide external parties with intelligence to assist them in attacking our system security. This could give rise to risk to our operations, and in turn the public-health benefiting research undertaken using our services. We would therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by maintaining the highest levels of security, which will enable the research undertaken using our data and service to continue.

- full details of any other linkage or anonymisation methods used when longitudinal records are assembled from data contributed by different healthcare providers;

The methods we have developed over time and at cost to our organisation for linking records, if disclosed could be used by other organisations to gain a competitive advantage, for reasons of commercial gain. We therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by preserving our ability to provide services which are to the benefit of public health.

- any assessments that have been performed of other potentially personally identifying information released to researchers in addition to encrypted patient and practice identifiers;

We are fully aware that anonymisation of healthcare data does not ensure that there are not circumstances under which data can be identified. That is why CPRD will operate under a whole series of activities to ensure, as far as is possible under legal contract that there are no misuse of data provided by CPRD.. However, we would emphasise that we have been providing data to researchers throughout the life of our predecessor service, GPRD, in a secure manner which has not given rise to any data security incidents throughout the life of that service.

- full details of statistical security and inference control mechanisms used to assess and control queries submitted interactively to CPRD by researchers;

The CPRD primary care data (and the previous GPRD primary care data) are made available to researchers in a range of different ways. This includes the provision of an online data access system. The data contained within this system do not contain any patient identifiers. Any pseudonyms which are used have no link to any identifiers within the dataset available to researchers. We have methods to assess the use of our online systems. However, the nature of such methods is such that their disclosure may provide external parties with

intelligence to assist them in attacking our system security. This could give rise to risk to our operations, and in turn the public-health benefiting research undertaken using our services. We would therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by maintaining the highest levels of security, which will enable the research undertaken using our data and service to continue.

- full details of the query audit mechanisms that will be used to detect abuse of non-interactive access after the fact;

We have methods to assess the use of the system and detect abuse. However, the nature of such methods is such that their disclosure may provide external parties with intelligence to assist them in attacking our system security. This could give rise to risk to our operations, and in turn the public-health benefiting research undertaken using our services. We would therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by maintaining the highest levels of security, which will enable the research undertaken using our data and service to continue.

- any technical assessments of the combined effectiveness of query auditing plus data perturbation, of the effect of data perturbation on the clinical dependability of perturbed data, and of any design trade-offs made between privacy and clinical dependability;

Data perturbation is not a technique used by CPRD on the basis that it is important for many types of public health research that the data remains as originally observed. We have other methods that we believe provide robust defence but the nature of such methods is such that their disclosure may provide external parties with intelligence to assist them in attacking our system security. This could give rise to risk to our operations, and in turn the public-health benefiting research undertaken using our services. We would therefore apply the exemption contained at S43 of the Freedom of Information Act. We feel that the public interest is best served by maintaining the highest levels of security, which will enable the research undertaken using our data and service to continue.

- copies of the agreements that CPRD users will have to sign to get access;

As the CPRD is a new service launched a matter of days previously, the legal agreements for supply of services to customers have not been finalised between us and our lawyers. However, it is likely that they will be based on those used for the supply of GPRD data. The previous GPRD data were supplied in the form of online access, single use datasets or commissioned research services. Copies of the standard agreement for each of these is enclosed.

- copies of any legal opinions sought by the MHRA on the legality of CPRD and in particular its compliance with DPA 1998 and with S8 ECHR;

See below

- any privacy impact assessments performed for CPRD.

Neither have been undertaken. However, we would emphasise that the services being offered by CPRD will build on those supplied by GPRD, which has been managed from within MHRA for the last thirteen years, during which time there have been no security incidents.

Annex C

-----Original Message-----
From: Ross Anderson [mailto:request-109883-2ea71462@whatdotheyknow.com]

Sent: 04 May 2012 12:04

To: MHRA Central Enquiry Point

Subject: Internal review of Freedom of Information request - Privacy mechanisms in CPRD

Dear Medicines and Healthcare products Regulatory Agency,

Please pass this on to the person who conducts Freedom of Information reviews.

I am writing to request an internal review of Medicines and Healthcare products Regulatory Agency's handling of my FOI request 'Privacy mechanisms in CPRD'.

I requested information on how privacy will be protected in CPRD and you refused this on the grounds that discussing your security mechanisms would be bad for security. This is wrong for at least four reasons.

(1) You submitted a paper "Privacy protection and research access mechanisms for National Health Service Data: The Clinical Practice Research Datalink" to the Journal of the American Medical Informatics Association, which contains much of the information which I sought and which you refused to disclose. The authors were Tim Holt, Tarita Murray-Thomas, Tim Williams and John Parkinson. I was sent the paper to referee, and made a number of criticisms of it, following which I understand it was rejected. I am not supposed to discuss the contents of this paper publicly because of the confidentiality obligation that I owe to JAMIA. However this is information which CPRD attempted to publish, and thus you cannot reasonably now argue that its publication would jeopardise security, expose their systems to attack and undermine the public health benefits.

(2) You cite cite s.43 as the basis for refusing to release material which you claim would imperil your security. But section 43 deals solely with prejudice to commercial interests and not with any of those matters.

(3) As a general proposition, the claim that discussing security mechanisms will endanger security is incorrect. There is a substantial research literature on this starting with Auguste Kerckhoffs in 1883 (see for example http://en.wikipedia.org/wiki/Kerckhoffs%27_principle; there is also a discussion in my textbook "Security Engineering").

(4) The government's Open Data "tsar", Tim Kelsey, promised at a public meeting in Cambridge, in response to a question from me, that the inference control mechanisms in use would be made public, as this was necessary not just for public confidence but for clinical safety. If, for example, data have been subjected to perturbation, or the trimming of extreme values, this may affect the conclusions to be drawn from them; and if de-identification is done by means of replacing name with postcode plus date of birth, then a researcher must consider the probability of misidentification (twins, students etc).

A full history of my FOI request and all correspondence is available on the Internet at this address:

http://www.whatdotheyknow.com/request/privacy_mechanisms_in_cprd

Yours faithfully,

Ross Anderson
www.ross-anderson.com

Annex D

From: Wilson, Stephen
Sent: 22 June 2012 16:04
To: 'request-109883-2ea71462@whatdotheyknow.com'
Subject: Internal review request for FOI 12/131

Dear Mr Anderson

Thank you for your email of 4 May 2012 requesting an internal review of the MHRA's decision to withhold certain parts of the information sought in your original request (FOI 12/131). I have now had a preliminary discussion with the answering Division regarding this matter.

I have not yet conducted a formal review as I wanted to try and clarify some points with you first.

Your initial request asked for the following information:

"…all the information you have about the privacy design for the Clinical Practice Research Datalink (CPRD) including

a) the threat model;
b) the security policy;
c) any assessments submitted to or performed by third parties including the ICO and CESG;
d) design documents for the privacy enhancing technologies in use or contemplated;
e) the design documents and evaluation reports for any trusted third party used for data linkage;
f) contracts with operators of trusted third parties and policy documents specifying the protocols to be used for record linkage, service level agreements, liability and audit requirements;
g) full details of how encryption will be used as a privacy enhancing technology;
h) full details of any other linkage or anonymisation methods used when longitudonal records are assembled from data contributed by different healthcare providers;
i) any assessments that have been performed of other potentially personally identifying information released to researchers in addition to encrypted patient and practice identifiers;
j) full details of statistical security and inference control mechanisms used to assess and control queries submitted interactively to CPRD by researchers;
k) full details of the query audit mechanisms that will be used to detect abuse of non-interactive access after the fact;
l) any technical assessments of the combined effectiveness of query auditing plus data perturbation, of the effect of data perturbation on the clinical dependability of perturbed data, and of any design trade-offs made between privacy and clinical dependability;
m) copies of the agreements that CPRD users will have to sign to get access;
n) copies of any legal opinions sought by the MHRA on the legality of CPRD and in particular its compliance with DPA 1998 and with S8 ECHR;
o) any privacy impact assessments performed for CPRD."

In our original reply

a) the threat model, and
b) the security policy

Were not answered as we sought clarification as to what you required. If you still wish to pursue this specific information, may I request that you supply this clarification either to myself, or to Mr Ford who provided the original answer and we will be happy to progress this for you.

The following questions appear to me to have been answered in the original request, but I would be grateful if you could confirm this for me, and that you were satisfied with those answers?

i) any assessments that have been performed of other potentially personally identifying information released to researchers in addition to encrypted patient and practice identifiers;
j) copies of the agreements that CPRD users will have to sign to get access;
k) copies of any legal opinions sought by the MHRA on the legality of CPRD and in particular its compliance with DPA 1998 and with S8 ECHR;
l) any privacy impact assessments performed for CPRD.

The following questions were all refused citing section 43 of the FOIA (commercial interests)

c) any assessments submitted to or performed by third parties including the ICO and CESG;
d) design documents for the privacy enhancing technologies in use or contemplated;
e) the design documents and evaluation reports for any trusted third party used for data linkage;
f) contracts with operators of trusted third parties and policy documents specifying the protocols to be used for record linkage, service level agreements, liability and audit requirements;
g) full details of how encryption will be used as a privacy enhancing technology;
h) full details of any other linkage or anonymisation methods used when longitudonal records are assembled from data contributed by different healthcare providers;
j) full details of statistical security and inference control mechanisms used to assess and control queries submitted interactively to CPRD by researchers;
k) full details of the query audit mechanisms that will be used to detect abuse of non-interactive access after the fact;
l) any technical assessments of the combined effectiveness of query auditing plus data perturbation, of the effect of data perturbation on the clinical dependability of perturbed data, and of any design trade-offs made between privacy and clinical dependability;

I have looked at the answers given and it is my belief that you are correct insofar as that the compromise of system security is not –in itself- a relevant consideration when considering Section 43.

However, in our response to those questions we said that we were unwilling to release information which could jeopardise the security of our systems, and that we would claim exemption under section 43 of the Act. We should have been clearer about the rationale for this statement, as we accept that section 43, in providing for exemption on grounds of commercial interest does not explicitly

deal with issues of security and confidentiality. The grounds on which we believe the exemption does apply are as follows:

- If we disclose under the Act detailed information about our security provisions, we would be placing into the public domain details about the methods we use to safeguard our data. In doing so we would be giving a direction to any parties wishing to maliciously attack our organisation. Any potential hacker or other malicious party would be provided with a first step on how to focus their attempts to circumvent our security provisions. We have sought guidance from the Agency's Senior Information and Risk Owner who has confirmed that she would not wish to release details of our security systems as to do so would inherently compromise security. Any party which was able to maliciously access our systems would place our business at serious risk, both in terms of business interruption and reputational damage. This in turn would have a significant negative effect on the viability of our business. As such we contend that our own commercial interests would be compromised by a release of information about our security systems.

- In a number of cases we have invested significantly in terms of both finance and effort in developing new systems. Were these to be placed into the public domain following disclosure under the Act, one of our commercial competitors could take advantage of our development work and set up competing systems. Without the cost of development which we have had to bear, such commercial competitors would be able to undercut our services and take a competitive advantage as a result of disclosure. This would compromise our own commercial interests, and we would therefore seek to apply the section 43 exemption in order to protect our interests.

In discussing our commercial interests we would also like to stress the nature of our business activities, both in terms of CPRD and its predecessor activity GPRD. CPRD and GPRD both exist to provide and support high quality research which is undertaken for the public benefit. All research undertaken using our data is protocol controlled and has to be authorised by the Independent Scientific Advisory Committee. A failure of our business model arising from disclosure of information following a request under the Act would prejudice this research activity and the benefit to public health which derives from it. To that extent we consider that the public interest is clearly weighted in favour of maintaining the exemption.

I have also discussed the issue of the JAMIA report with the answering Division and, following that discussion, we see no reason why this cannot now be disclosed to you (please find attached)

If you are satisfied with this reply, I will conclude the internal review process at this stage. However, should you remain dissatisfied with the Agency's response I will formalise the review and send you a copy so that you can, if you wish, escalate the matter to the Information Commissioner's Office.

Kind regards

Steve Wilson

FOI Officer
Policy Division
MHRA - 020 8030 6852

Annex E

-----Original Message-----

From: Ross Anderson [mailto:request-109883-2ea71462@whatdotheyknow.com]

Sent: 05 July 2012 15:02

To: Wilson, Stephen

Subject: Re: Internal review request for FOI 12/131

Dear Stephen,

Thank you for the Holt paper.

When building a secure system, the standard procedure is to first write down a threat model, which is typically a list of the bad things against which you want protection. In the case of an anonymised medical record system, this might include theft of copies of anonymised data, for example when a laptop is stolen from a hospital (as in the June 2011 London Health Programmes case); dishonest insiders (such as when Dr Andrew Jamieson accessed celebrity records on the Scottish Emergency Medical Record); and an academic publishing a means of re-identifying your records (see for example the work of Latanya Sweeney).

The second step is to develop a security policy, which states how the documented threats are to be mitigated. For example, the HIPAA regulations in the USA typically require that de-identified data be such that no more than 0.04% of patients can be reidentified, while "differential privacy" requires that none may be, even in the face of adaptive queries of the database by an opponent. These terms are explained and illustrated in much greater detail in standard textbooks such as my own "Security Engineering" book (available online at http://www.cl.cam.ac.uk/~rja14/book.html).

The first two parts of my freedom of information request thus seek the documentation you assembled (including meetings of minutes you held) to assess what the threat would be to your system, and the top-level strategy you adopted in order to manage the resulting risks. You talk later in your email about business interruption and reputational damage. The assessment you carried out of that should be part of the threat model.

Next, you refuse to release any details of how the security policy was implemented by means of inference control mechanisms, audit procedures and other protections, making a "security-by-obscurity" argument that "We have sought guidance from the Agency's Senior Information and Risk Owner who has confirmed that she would not wish to release details of our security systems as to do so would inherently compromise security."

The strong consensus of security professionals is that this "security-by-obscurity" argument is wrong in general and does not apply in most cases. Again, my book has much further detail, but for historical background, obscurity was first dismissed by Auguste Kerckhoffs in 1883; the principle that "the enemy knows the system" was restated by Claude Shannon, father of information theory and a top US cryptanalyst, in the 1940s. With the greatest of respect, it is not appropriate for a mid-level civil servant who presumably has no professional

expertise in the subject to think she knows better. Indeed, there is a long history of people relying on security systems with obscure designs that failed catastrophically because of weaknesses that would have been immediately obvious on public review. If you persist in refusing to disclose the statistical security mechanisms on which we are all as patients expected to rely for the privacy of our health information, then I will appeal this to the ICO and if need be the Tribunal.

The same applies for any evaluations you have had done on the statistical security mechanisms, whether by an outside consultancy or by an internal government body such as CESG. If you have had no evaluation done, that is disgraceful and a matter of public interest; if you've had an evaluation that gave you a clean bill of health, you have no reason to withhold it.

Finally, I'd like to remind you that Tim Kelsey did undertake at a public meeting on 8 September 2011 that the statistical security mechanisms would be open to public review.

Yours sincerely,

Ross Anderson
www.ross-anderson.com