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 fra 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.