

Connecting for Health: Controllers “in Common”.

Dr Paul Thornton MPH, FRCGP
January 2008

The purpose of this paper is to discuss the concept of “Data controllers in common” in relation to the NHS National Care Records Service (NCRS) and their plans for obligatory sharing of clinical records with researchers, managers and other local and national government departments.

Clinicians, researchers and health service managers might all legitimately aspire to complete, accurate and comprehensive information about patients. In a benign world those aspirations might be met. But in the real world, none of us have ever enjoyed such luxury. Aside from the consultation skills and specialism of the clinician, the information received is dependent upon the patient

- (a) presenting to clinicians for care and,
- (b) trusting that their own vulnerability will not be increased by divulging that information.

The notion of balancing a conflict between good data analysis on the one hand and proper observation of data protection laws on the other is fundamentally flawed. Rather than a barrier, patient control over data and confidentiality is a prerequisite to the collection of good quality data from as many patients as are willing and thereby allowing good research and good management, as well as good care for that individual.

Connecting for Health’s own risk benefit analysisⁱ showed that the health gains from sharing information in the manner they propose were outweighed by the health losses arising from patients being inhibited in their information sharing with clinicians.

The General Practitioners Committee (GPC) has been entirely correct to press for the General Practice Systems of Choice (GPSOC)ⁱⁱ initiative to avoid practices being pressured into needlessly changing their established and successful clinical software. GPSOC has been an important concession. It is understandable that the GPC may have wanted to press on and consolidate that concession. With “GP2GP”, the direct electronic transfer of entire records when a patient changes GP, there is tremendous potential to realign some of CfH’s more unrealistic expectations and to develop systems that will work, particularly where there is great need in hospitals.

Regrettably, levers remain that could pressure GP’s to change to systems preferred by their Primary Care Trust or more particularly CfH Local Service Providers.

Firstly GP’s have to sign up for GPSOC or else they will be obliged to transfer to the default local PCT chosen system

A second lever is the spurious claim that if GP’s do not migrate to a single system within a locality the care of their patients will suffer. The proposal is that *detailed* care records, not just the *summary* care record, created within all services in a locality will be mutually accessible. It needs to be understood that a “locality” may be the size of a large city.

A small number of health communities using TPP System One may have jumped the gun in this regard by proceeding to local cross-organizational common databases without the safeguards that even Connecting for Health has described as essential to fulfill common law obligations, particularly patient controlled “sealed envelopes”.

Patients will commonly receive care from professionals across the boundaries between such health communities, not least across the London/Home counties borders. Rapid targeted electronic communication of relevant and necessary detailed information between such professionals will be needed and such mechanisms would similarly suffice for care communications within “localities”.

However, GPSoC is not sufficient to ensure privacy and confidentiality standards previously demanded by GPC/BMA¹. Even with GPSoC participation, users from other provider organisations could still be able to access General Practice *detailed* care records as a common shared database.

CfH proposals, even with GPSoC, still need further development to meet legal and ethical considerations. Central to these are the concept of “Data Controllers in Common”.

In an early proposal for the “new” GP contract, the Department of Health (DH) tried to include a clause such that GP’s would be data processors on behalf of the NHS, rather than independent data controllers. On challenge the suggestion was rapidly removed but ever since, there has been uncertainty about who would be the “data controller” for information recorded on the NCRS.

Parliamentary questions submitted by Mr Jeremy Wright MP have recently secured answers from Mr Ben Bradshaw MP, Minister of State, (10 December 2007) who advised that

*“With regard to **detailed** care records provided as part of the National Health Service care records service, the Department is data controller in common with the NHS organisations providing health care to patients.ⁱⁱⁱ”*

And

“The data controller for information held within the secondary users service is the Department. Other organisations lawfully permitted access to data held within the secondary users service will be data controllers in common for the subset of data that they can access.^{iv}”

The concept of “data controller in common” derives from the first paragraph of the Data Protection Act

“data controller” means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;^v

Through Internet searches of public documents, I have been unable to locate prior references to “Data controllers in Common” in respect of NCRS, except a minute of the Council of Caldicott Guardians with regard to the Children’s Database “Contact Point” which will store and share information from NCRS identifying agencies and professionals who are involved in the care of the child to all other agencies and professionals.

“Access control will be through the local authority and therefore agreements need

¹ BMA ARM/Conference of LMC policies.

to be made with Councils with Social Services Responsibilities (CSSRs).

However, the organisations adding data will be data controllers in common within the terms of the Data Protection Act 1998.”^{vi}

There is minimal elaborative guidance about, or for, “data controllers in common” on the information commissioner’s website.

“The determination of the purposes for which, and the manner in which, any personal data are, or are to be, processed does not need to be exclusive to one data controller. Such determination may be shared with others. It may be shared jointly or in common. “Jointly” covers the situation where the determination is exercised by acting together equally. “Determination in common” is where data controllers share a pool of personal data, each processing independently of the other.”^{vii}

Solicitor Gillian Howard^{viii} describes “Data controller in Common” thus

“Data controllers who share personal data on data subjects for different purposes are referred to as data controllers in common. Each data controller remains individually responsible for the processing they have carried out on the data.

Data controllers who share information on data subjects for the same purpose and who would be jointly liable for any breach under the DPA are referred to as joint data controllers. “

I have found it difficult to identify other examples of data controllers in common. Indication of such commonality is not a requirement of the Data Protection Register.

The biggest example of “Data Controllers in Common” seems to be the Police National Computer (PNC), for which the Data Controllers are the various Chief Constables . It is noteworthy that the Home Secretary/Home Office is not a data controller for the PNC. It begs the question whether the SoS for Health should ever be a “data holder in common” for active clinical health records. Connecting for Health functions might reasonably be fulfilled by functioning as data processors strictly to the mandate of the Data Controllers responsible for the primary collection and recording of data. There are powerful civil liberties arguments for the notion that the secretary of state should never be a data controller in common.

If one accepts the concept of “Data Controllers in Common” for the National Care Records Service, then one is accepting that any and all data recorded in a detailed care record created by any clinician is shared. The fundamental distinction is that a “data controller in common” is able to process information recorded by other data processors without referring back to the source data controller who originally recorded that information. Physical or electronic control of that processing by the source controller and the controls available to the patient, via the source controller, are diminished. The data in common will include data that is recorded in “sealed envelopes” or that the patient has otherwise dissented from inclusion in the summary care recorded, or that the patient has otherwise indicated should not be released beyond the clinical team to which it is divulged.

“Controllers in common” (which includes all their employees) are obliged to process the information lawfully. Data controllers in common could agree between themselves the nature of the processing and any restrictions of that processing by that data controller. However, the

application of the law and of any such agreement becomes dependent upon a clear uniformity of interpretation. Such a consensus does not exist.

While each data controller is remains individually responsible for the processing they or their employees have carried out on the data, this could not exempt the source controller from liability if the initial act of recording data on a system that has data controllers in common is not itself lawful. Indeed that initial recording may be the only unlawful component in a chain of otherwise lawful processing.

The provision of explicit consent for the recording of information to the summary care record would be demonstrably lawful and GPC policy should not compromise that as a requirement. It is possible that proposals for the summary care record might be lawful if (a big if) one accepts that the requirements set out in advice from the MDU are fulfilled. This demands a high standard in respect of acceptable implied consent for the formation of a summary care record using prescription and drug allergy data, and there is subsequently a requirement for explicit consent for the maintenance of that summary care record and any additions. Presented as “concessions” by departing health minister Lord Warner these safeguards are legal requirements.

The same requirements in law for the *summary* care record should apply to detailed care records recorded on the NCRS system because it is now confirmed that *detailed* care records will be directly accessible beyond the employees of the data controller to whom information is first divulged.

Access controls permit this. Sealed envelopes are not yet developed, may not work and **will be over ridden by staff from outside the practice**. Detection of infringements through audit trails are retrospective, and the audit trail itself is intrusive and sensitive as it will document all the health care professionals who have legitimately been dealing with an individual. Specialists in genito-urinary medicine do not treat sunburn.

While clinicians are under an obligation to make a record of a consultation, there is no obligation that such a record be created on the NCRS, and there is certainly no obligation that such a record be created without the consent of the data subject and there is an unequivocal common law, privacy right and/or DPA section 10 requirement to respect for patient dissent.

The concept of “data controllers in common” needs to be clearly understood to be distinct from the functioning of independent data controllers who, as now, share information through the transfer of selected data from the control of one to the independent control of the other. Some data is shared but it is not the same “pool of data.”

It should also be discriminated from the situation where a separate legal entity functions as a “data processor”. In such circumstances, the third party must only process the information in accordance with the mandate of the data controller.

“Processing” includes deleting and amending, as well as transferring and searching data. It could be possible for a data controller in common to process records that they did not create without actually viewing the data in identifiable form, thereby fulfilling the letter, if not the spirit of the Care Records Guarantee. There is a need for clarity with regard to who will be able (and not just “allowed”) to process information in ways other than simply viewing it. The risks to data quality arising from common data shared with environments are substantial.

There is unequivocal debate with regard to the lawfulness of Connecting for Health proposals and that debate is undiminished by the use of the superficially expedient concept of “Data controllers in common”.

Each provider within the NHS remains an independent legal entity and has sole obligations before the data is recorded on the shared database. The unconsented recording of information on a common, shared detailed care record database is likely to be unlawful.

Ben Bradshaw has acknowledged that CfH proposals do not meet existing EU law requirements as set out in a paper produced by the “Section 29 Working party”, made up of Data Protection Commissioners from across Europe. In a letter to the BMA^{ix} dated 26 September 2007, Mr Bradshaw endeavours to diminish the importance of that document by describing it as no more than a “working document”.

In the same letter Mr Bradshaw confirms his previous refusal to meet a BMA request to release the legal advice that has been provided to the department of healthⁱⁱ. A subsequent request under the Freedom of Information Act has been submitted and rejected and is currently under appeal^x. Until that advice is published in full how can there be trust or concordance between any “Data Controllers in Common” with regard to what is or is not lawful?

At the very least it should be noted that the CfH/DH have previously described metaphorical “sealed envelope” software as essential to fulfil common law confidentiality requirements. Despite several years of aspiration, the Health Select Committee recently elicited that the specification for sealed envelopes was only provided to contractors in April of this year. Dr Simon Eccles has undertaken to provide the specification to me but it has not yet been received.

General Practitioners familiar with established GP systems will be amazed to learn from a further parliamentary answer from Mr Bradshaw that “*Sealed envelope requirements have been developed in consultation with GP’s and reflect existing security mechanisms found in the main established GP systems. The sealed envelope functionality does not require new or innovative software to be developed for GP systems but will require compliance testing with the spine when this functionality is available in mid 2008*” There is no clarification of why software that he claims to be so established already should take more than 12 months to implement from the provision of the specification.

Further, of particular concern, it is intended that patient information will be taken from detailed care records about all patients in a wholly identifiable format and stored in the national secondary users database. It will be released to some users in an identifiable format. For other users it will be released after a reversible “pseudonomising” process. Even the Patient Information Advisory Group (PIAG), the body set up to approve the release of patient data without consent has expressed concern about the lawfulness of proposals for the pseudonimisation process used by secondary users service^{xi}.

ⁱⁱ A previous paper(a) by the author was submitted to the Department of Health by the BMA as part of the considerations by Lord Warner’s ministerial working party. A counsel’s opinion was obtained by the DH in response to that document. Assurances of lawfulness based on that advice were made in respect of the Summary Care Record when a full opt out was conceded (b). However, no such explicit claims were made in respect of the remainder of CfH proposals.

(a) <http://www.ardenhoe.demon.co.uk/privacy/NHS%20database%20proposals%20unlawful.pdf>

(b) <http://www.ardenhoe.demon.co.uk/privacy/decoy.pdf>

Data transfers to and from SUS are intended to include the free text components of read coded data entries. For many practices, this will include identifying text from scanned correspondence. It is also likely that SUS data will also include identifiable data in the form of attached image files of scanned documents, photographs or files generated by non-core technical software e.g. ECG recordings. This identifying data, which may be about third parties with not be stripped out by the pseudonimising process.

Mr Bradshaw has also confirmed that it will be possible for the Secondary Uses Service data to be searched to identify individuals who meet specific criteria. While some safeguards apply this represents a fundamental shift compared to current procedures for police access which usually starts with the established identity of a specific patient. Function creep will result in the Secondary Users Service being searched to identify possible suspects.

A recent report about SUS by the Care Record Development Board acknowledges the requirements for consent or true anonimisation that the law requires, but then applies that law at the wrong interface. The law should be applied at the interface between the clinician and the secondary users database. The intention is to apply it at the interface between the secondary users database and some of its data recipient clients.

While each data controller is remains individually responsible for the processing they or their employees have carried out on the data, this could not exempt the source controller from liability if the initial act of recording data on a system that has data controllers in common is not itself lawful.

Recent events.

The loss of the HM Revenue and Custom data discs occurred on the 18 October 2007.

The Prime Minister made a speech on Liberty^{xii} on the 25th October 2007. Despite government policy in this regard having previously been hugely positive towards information sharing between departments, the prime minister referred extensively to privacy risks and initiated a review of information sharing between government databases by the Information Commissioner and Dr Mark Walport of the Wellcome Trust^{xiii}.

The Chancellor of the Exchequer advised parliament that he was not informed of the missing discs until Saturday 10th November^{xiv}. He advised that the Prime Minister was informed half an hour later.

On the 17th December 2007, the House of Commons Justice committee published a report^{xv}, "Protection of Private Data". Based substantially upon evidence provided to the committee by the Information Commissioner, Mr Richard Thomas, on the 4th December, the report also drew heavily on the Speech made by the prime minister.

The following exchange is pertinent.

Q16 Dr Whitehead: Before all this most recent series of events occurred, the Government had published an Information Sharing Vision Statement, in September of last year, and in that, among other things, they stated: "The existing law ensures that appropriate safeguards will be maintained on the sharing of medical, taxpayer and criminal records information in particular. But within that law, it is possible for there to be greater information sharing than currently occurs -- and this can be combined

with proper respect for the individual's privacy." It looks a little dated now, does it, do you think?

Richard Thomas: I think it does, yes. Perhaps it looked a little bit dated when it was published. We noted the Vision Statement from the Ministry of Justice, and we had some reservations about that. We saw it at one stage in draft, and we made some suggestions for improving it, but I think at that time, there was perhaps too much faith in the benefits of information sharing. If I can just read from the introduction to that statement: ". . . the Government is committed to more information sharing between public sector organisations and service providers." It went on to say: "We recognise that the more we share information, the more important it is that people are confident that their personal data is kept safe and secure." But we thought that was perhaps not the end of the story. Since then, we published what we call our Framework Code of Practice for sharing personal information; this is quite a detailed code which we have been urging on public bodies for where they are sharing information, when there is a good reason to do so. Above all, that is the important thing, first of all, to identify why you are collecting and sharing information, and then make sure that you stick within that particular remit. But if you do need to share from one organisation to another, our Framework Code is meant to provide a template for more detailed codes in particular situations. That has a page on the importance of taking security very seriously, and it elaborates the legal requirement which I shared with you earlier. The vision statement, I think, is also a bit dated, because since then, on 25 October, the Prime Minister made his, I think, very important speech on Liberties, and that included some three or four pages on privacy and data protection.

Despite being devoted to data sharing, the "Framework Code of Practice"^{xvi} makes no reference to the concept of "data controllers in common". However it does describe a number of matters that are not resolved in the context of CfH proposals.

Particularly, those matters are not addressed in the draft contract^{xvii} between General Practitioners and Primary Care Trusts in respect of GPSoC. This simply includes a section which restates the legal obligation on both parties to process the data lawfully and indemnifies each party from unlawful activity undertaken by the other. This is somewhat tautologous and affords little protection to either PCT's, Provider trusts or General Practitioners.

In conclusion, the concept of "data controllers in common" may not exacerbate established concerns in ethics and law with regard to long described CfH proposals. However, it should be accepted that the concept is not sufficient to render information sharing lawful or ethical. Recent new guidance from the information commissioner demands review of the proposals. In addition, several reviews of government information handling are on going in the wake of the HMRC data loss and there should be no further binding commitments to CfH proposals until those reports are published and properly considered.

Finally, it is not sufficient for Connecting for Health or General Practitioners to interpret patient mandates that have already been received as relating only to the Summary Care Record. Such patients have asserted their right that their records are not recorded on National systems. The 93c3 Read code will enable such patients to be identified by the practice. CfH intends that the code will ensure that such records cannot be viewed as summary care records but it is not clear that this will prevent access that is external to the practice, by means of the national systems, as described above.

Dr Paul Thornton MPH, FRCGP
Pear Tree Surgery
28 Meadow Close
Kingsbury
Warwickshire
B78 2NR
paulthornton@beeb.net

Version 2: Correction of typo's & broken links.

ⁱ <http://www.nhsconfidentiality.org/wp-content/uploads/November%20-%20NHS%20Care%20Records%20Report.pdf>

ⁱⁱ <http://www.connectingforhealth.nhs.uk/systemsandservices/gpsupport/gpsoc>

ⁱⁱⁱ <http://www.theyworkforyou.com/wrans/?id=2007-12-10b.169025.h&s=section%3Awrans+speaker%3A11791#g169025.q0>

^{iv} <http://www.theyworkforyou.com/wrans/?id=2007-12-10b.169023.h&s=section%3Awrans+speaker%3A11791#g169023.q0>

^v http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_2#pt1-l1g1

^{vi} <http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott/meetings>

^{vii}

http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_act_legal_guidance.pdf

^{viii} Vetting and Monitoring Employees: A guide for HR Practitioners. Author Gillian Howard
http://books.google.com/books?id=w_txK7369CQC&pg=PA92&lpg=PA92&dq=%22data+controller+in+common%22&source=web&ots=pQ8oij_Hg4&sig=MilhWPh8g89wfZHik2OFO5vd0RA#PPA92,M1

^{ix} <http://www.ymcentre.freemove.co.uk/download/bbresponse.pdf>

^x http://www.ardenhoe.demon.co.uk/Bradshaw%20correspondance/PT_LD_01_12_07.pdf

^{xi} <http://www.advisorybodies.doh.gov.uk/piag/piagresponse-CRDB-SUS.pdf>

^{xii} <http://www.pm.gov.uk/output/page13630.asp>

^{xiii} <http://www.justice.gov.uk/reviews/datasharing-intro.htm>

^{xiv} http://news.bbc.co.uk/1/hi/uk_politics/7117291.stm

^{xv} <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf>

^{xvi} http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf

^{xvii} <http://www.connectingforhealth.nhs.uk/systemsandservices/gpsupport/gpsoc/news/pctpractice.pdf>