

The NHS Database: Lord Warner's opt out decoy.

A review of persisting privacy and confidentiality issues.

Dr Paul Thornton MPH, FRCGP.

March 2007

Introduction.

10

As a parting shot just before Christmas, resigned Health Minister Lord Warner generated extensive press coverage by announcing unequivocally that patients would be allowed to keep their information off the national database that is being created by Connecting for Health, the Department of Health's IT wing. This was trumpeted as a substantial concession in response to letters sent to the Department of Health by patients. It appeared that Lord Warner belatedly recognized the political and ethical obligations on the Department of Health (DH) – obligations that were increased by the editorials and comment from newspapers across the political spectrum once they came to understand what the NHS had otherwise been trying to do¹.

20

Lord Warner's announcement was trailed by Mr Harry Cayton in an interview with The Guardian². The newspaper had previously printed a proforma letter that was sent to the Department of Health by readers. Mr Cayton is "National Director for Patients and the Public" at the Department of Health, a political appointment dubbed "Patient's Tsar". Mr Cayton is also chair of Connecting for Health's "Care Records Development Board". So he should know.

So far so good. But....

30

It is nearly two years since Mr Cayton previously reassured on BBC TV news³ that patients would be able to opt out of the national database entirely if they so choose. Despite the gestation period of an elephant, the board he chairs has failed to amend the National Care Records Guarantee to inform patients of that choice and how it can be exercised. Nor has the board given any indication of how the care of such patients might be taken forward if they are ever able to exercise that choice.

And there lies the uncertainty about Lord Warner's reassurance.

40

Mr Cayton was also the chair of a "Ministerial taskforce"⁴. That task force had reported to Lord Warner on the 6th of December and the later publication of the report provided Lord Warner with the opportunity for his reassuring announcement. Unfortunately, the detail of the working party report and the reassuring announcement by Lord Warner are mutually incompatible.

1 Are medical secrets up for grabs? BMJ 2007;334:16-17 (6 January) <http://www.bmj.com/cgi/reprint/334/7583/16-a>

2 Guardian December 16 2006 "How patients' protests forced a rethink on NHS computer records" http://www.guardian.co.uk/uk_news/story/0,,1973239,00.html

3 See video link off <http://news.bbc.co.uk/1/hi/health/4392555.stm>

4 Report of the Ministerial Taskforce on the NHS Summary Care Record http://www.connectingforhealth.nhs.uk/publications/care_record_taskforce_doc.pdf

Lord Warner somehow concurrently accepted the report and their recommendations while his interviews, and the headlines he precipitated, have given the public to understand that there is an opt out from the entire national database. Where lies reality?

50 The Department of Health intends that everyone's data will be stored on the national database.

But this is to accept that it is a decision which rests with the DoH. The NHS is made up of numerous separate legal entities each of which is an independent registered data holder with enforceable obligations under the Data Protection Act. There is no mandate for those data holders to transfer patient information onto the National Database. There is certainly no obligation to transfer identifiable data contrary to the wishes of the data subject. Patients are asserting their rights to confidentiality, data protection and privacy. There are better ways to develop IT in the National Health Service.

60

Ministerial task force report

The taskforce report is explicit. Everyone is expected to have their information recorded on the national database. Neither an "opt in" nor even a true "opt out" choice is intended.

And this is despite the task force including senior representatives of the British Medical Association and the Royal College of General Practitioners. The policies of their respective organisations that demand an informed "opt in" from each patient before their information is placed on the database.

70

In an appendix, the Ministerial task force report documents many unresolved basic privacy considerations. Set up to resolve these concerns, the hands of the working party were tied from the outset in their terms of reference;- *"to resolve the ethical and practical differences over the implementation of the shared summary record and to devise a programme of work for its implementation, within agreed policies (sic), for the benefit of patients and the NHS."*

These matters cannot be resolved unless "agreed policies" are changed. The policies are only "agreed" because the Department of Health entered in to contracts with suppliers in a secret process without consultation.

80

Summary care record

All that is being offered by the ministerial working party is an "opt out" from the "summary care record". This limited opt out is important because all information in the summary care record will otherwise be accessible to all NHS staff nationally⁵.

Initially the summary care record will include only current medications, allergies to medication and adverse reactions. This is sufficient information to imply highly sensitive diagnoses. If you know the treatment you know the disease. It is intended that the summary care record will include even more data as time passes. The

90

⁵ Staff will not be *allowed* to access records unless a "legitimate relationship" exists, but they will be *able* to access records. It will have to be a rapid and easy process to create a "legitimate relationship" (whether or not it is authentic) else the justification for the service – care in an emergency – will be unworkable.

summary information will initially be generated from data currently held by General Practitioners on their discreet and discrete systems.

But this limited opt out is not sufficient

Detailed care records

CfH intend that **all** clinical, psychological and social information will be recorded by professionals in a “Detailed Care Record”, a subset database of the entire scheme. The information will be stored on centralised computers that are remote from the unit treating the patient⁶. A single individual should therefore have a different “Detailed Care Record” created by each NHS unit by whom they are being treated. Previous CFH documents⁷ confirm that detailed care records will certainly be accessible by all staff who work in the same NHS unit as the professional to whom private information has been divulged. This may be as small as a single GP practice or as large as an NHS Trust covering 2 or 3 District General Hospitals.

In addition, enormous numbers of staff in all the units which share the same I.T. infrastructure, described curiously as an “*instance*”, will have the ability to access the detailed care records created in those other units in that “instance”. Connecting for Health (CfH) have divided health services in England into five geographical areas, called “clusters”. Each cluster database may be divided into as few as two or three “instances”. The number of staff and patients served by a single “instance” will be huge.⁸ Users of an “instance” will be widely spread geographically. Some restrictions might be placed on who is “allowed” to access the records but this is substantially exceeded by a recognition of the numbers who are “able” to access the records. The biggest security risk to any large database arises from illegitimate use by staff with at least some degree of legitimate access.

At the planning stages of the project, Connecting for Health reassured that patient information would be protected from widespread inappropriate sharing because software would be used to hide sensitive information that patients did not want revealed, even to other health professionals. The proposals were metaphorically dubbed “sealed envelopes”. These proposals were described even by CfH as necessary to meet the project’s legal obligations on privacy and confidentiality. After substantial delay and failure to produce working software in this regard, CfH

⁶ It is a valid debating point that medical data might be better protected if it was stored on servers located in Germany! Having experienced the subversion of medical privacy in it’s modern history not only does Germany have more stringent standards for medical privacy, but those laws are more appropriately enforced.

⁷ Paradoxical Access
<http://www.ardenhoe.demon.co.uk/privacy/Paradoxical%20access.pdf>

⁸ At the same time it was revealed, that health professionals who do not work in the same “instance” will never be able to share access to “detailed care records” even if they are directly involved in the care of the patient and the patient consents to that information being shared. This will be a particular issue when the GP is in one locality and the hospital is in another. It rather defeats the explicit objective of the national database proposals. Even if the CfH proposals go ahead as planned, additional messaging mechanisms will be required to ensure the proper transmission of information about patients whose care transcends the boundary between “instances”.

documents have just been updated⁹. It is confirmed that all the inadequacies¹⁰ in the proposals persist.

- The software is not yet written or tested
- It will not be available until long after the database is up and running so that detailed care records will be unprotected
- 130 • It will not protect information that is stored in scanned images of historical documents.
- The patient controls can be over ridden
- The sealed envelopes will be ignored in respect of information transferred to the Secondary Uses Service (see below)

Through a further safe guard, “Role based access”, it is intended that staff will only be able to access information that is justified by their job purpose, as indicated when they log on using their chip and pin card. This simplistically implies that information can be divided clearly into administrative information that is sufficient and safe for receptionists, ward clerks and secretaries to access, while other sensitive clinical information only needs to be seen by doctors. It is just not that simple. The proposal is untested. Already, a Warwickshire hospital A&E department has abandoned the use of chip and pin cards by individual users because they were unable to log on and off quickly enough.¹¹ Warwickshire primary care trust is enabling administrative staff who work at the PCT to be issued with Chip and Pin cards that would misrepresent these staff as employees of the local General Practitioners, thereby allowing access to sensitive patient information¹².

Healthspace

150 Despite previous reassurance from Ministers about the importance of access controls being based on secure “chip and pin” cards, the ministerial working party appear to accept that the summary record *for every patient* will be placed on a public website, “Healthspace”, that will be accessible without such cards over the internet. Even the banks give customers a choice over whether or not they have an internet account!

Perversely, it is claimed that this will enable patients to review their records before deciding if they want their data to be released on to the nationally accessible NHS summary care record. This is putting the cart before the horse.

160 The author discussed the “Healthspace” proposals with some of it’s leading GP protagonists at the recent user group conferences for the InPS Vision and the EMIS GP software systems. There is concordance with the objective of sharing information more fully with patients. But clinicians also acknowledge that many patients would be

⁹ “Sealed Envelopes” Briefing Paper: “Selective Alerting” Approach
http://www.connectingforhealth.nhs.uk/crdb/sealed_envelopes_briefing_paper.pdf

¹⁰ Why might National NHS database proposals be unlawful?
<http://www.ardenhoe.demon.co.uk/privacy/NHS%20database%20proposals%20unlawful.pdf>

¹¹ NHS security dilemma as smartcards shared. Computer Weekly 30th January 2006
<http://www.computerweekly.com/Home/..%5CArticles/2007/01/30/221461/nhs-security-dilemma-as-smartcards-shared.htm>

¹² <http://www.computerweekly.com/Articles/2007/02/27/222069/smartcard-scheme-makes-a-nonsense-of-it-security.htm>

obliged by peer, social, familial, financial or intimidation pressures into providing copies of, or access to, their internet record if the possession of a “Healthspace” record was to become standard. Parents of adolescents, employers of their staff, “friends” of the elderly and abusers in domestic violence will all want access. “Health space”, as proposed, is a major threat to patient privacy.

170 It is clear that patients the creation of an internet record should require consent to in the first place and that the Healthspace record must be invisibly editable at the request of the patient by clinicians *before* it is placed on the internet and at any stage subsequently. The most vulnerable in a society have the greatest difficulty protecting their right to privacy.

“Healthspace” type proposals were the lowest IT related expenditure priority for patients in the 2002 Which? public opinion poll report¹³ commissioned by the NHS Information Authority at the outset of this project.

180 **Secondary Users Service (SUS)**

Just days after Lord Warners announcement, Connecting for Health instructed mental health units to start placing identifiable information about all their patients on the national database from March of this year¹⁴. Eventually, unrestricted patient information will be siphoned off into this component of the national data structure known as the “Secondary uses service”.

“The vision for the Secondary Uses Service is to capture, process and enable access and reporting on all data relating to NHS commissioned activity.”¹⁵

190

The Secondary Care Service relates to the use of information other than for the direct care of the individual to whom it relates. Generally,

- Research, the evaluation of care (clinical audit) and infectious disease prevention
- Management of health services
- Payment to organisations for care provided.

200

Approved Users of this data may be from within the NHS or outside in the civil service or in universities and the pharmaceutical industry. A recent report¹⁶ for the Chancellor of the Exchequer commends *“the use of the National Program for IT to identify appropriate patients for clinical trials.”*

¹³ http://www.connectingforhealth.nhs.uk/publications/share_with_care.pdf

¹⁴ Secondary Uses Service: MHMDS Implementation Guide for the NHS to support NWCS Replacement Version 1.2 23/10/06
www.connectingforhealth.nhs.uk/sus/reference/mhmlds_implementation_guide.pdf

¹⁵ Secondary Uses Service: Strategic direction. Document record ID Key NPFIT-FTN-TO-BAR - 0009.02 http://www.connectingforhealth.nhs.uk/sus/reference/sus_vision.pdf

¹⁶ A review of UK Health Research funding. Sir David Cooksey December 2006 http://www.hm-treasury.gov.uk/media/56F/62/pbr06_cooksey_final_report_636.pdf

Connecting for Health have previously reassured that the transfer of Secondary Uses Service data would be anonymised. Recently confirmed CfH documents^{15, 17} however reveal that patient information will be

1. collected and stored individually in an entirely identifiable form, and
2. will be searchable, and
3. will not be anonymised when released to end users of the Secondary Uses Service.

210 Information will be provided to some end users in a fully identified form. It will be provided to others in a form which is described as “Pseudoanonymised”. As the term implies this is a compromise. Information is stripped of its obvious identifiers – name, address, date of birth etc but replaced with a unique number. The purpose of pseudoanonymisation is to prevent data about the same individual being entered twice on the same data base from separate sources but it also enables data to be tracked back to its original fully identified structure. Proposals to supply wholly anonymised and aggregated patient information, which would be suitable for the majority of essential NHS business functions seem to have been dropped.¹⁸ This would include invoicing & payment arrangements for the “Payment by Results” internal market. There is
220 certainly no intention to anonymise information at its source i.e. when it remains under the control of the registered data holder who has care of the patient and to whom the information was initially divulged in confidence.

Patient information on the Secondary Uses Service, will be under the control of the Department of Health and apparently outside the control of both patients and the clinicians in whom it has been entrusted. A concealed, background, duplicate national database of identifiable medical records.

230 The Secondary Uses Service will be provided under contract by an American multinational company called McKesson and by British Telecom.

The proposals for the Secondary Uses Service are already well advanced as adaptations of established data flows¹⁹. The Patient Information Advisory Group recently acknowledged that “*Much of the current NHS activity involving access to and use of patient identifiable data has no clear or secure basis in law. This includes data from the Clearnet DataStream by NHS staff not directly involved in providing care to patients.*”²⁰

240 But to quote the planners for the Secondary Users Service, “*it is important to understand that this is much broader than a replacement for the NHS-Wide Clearing service. These data will be provided as a by-product of the NHS Care records service and other connecting for health programmes such as choose and book and the electronic transfer of prescriptions. These data will cover all care settings (so*

¹⁷ [The SUS Data Handling Protocol](#)

http://www.connectingforhealth.nhs.uk/sus/reference/sus_data_handling_protocol_feb.pdf

¹⁸ SUS Pseudoanonymisation pilot: Draft testing strategy for test 1 of 4 Draft version 6 7th July 2006
http://www.connectingforhealth.nhs.uk/sus/reference/pseudonymisation_pilot_testing_strat.pdf

¹⁹ <http://www.connectingforhealth.nhs.uk/news/sus-replaces-decommissioned-nwcs-clearnet-service>

²⁰ The use of patient information in the Long Term Conditions programme.
<http://www.advisorybodies.doh.gov.uk/PIAG/piag-ltc-nov2006.pdf>

primary and community care as well as acute) ...including all those services provided for the NHS by the independent sector.”⁴

Information will be taken from summary and detailed care records. Information that has been “sealed” or “sealed and locked” using the metaphorical sealed envelope software will not be protected from the Secondary Uses Service.

250 **Choose and Book, ETP and ? GP2GP**

The CfH electronic referral system, “Choose and Book” (C&B) and the “electronic transfer of prescriptions”(ETP) have been perceived by the medical profession as messaging services. They are understood to replicate established and patient informed confidential information flows for direct clinical care. The knowledge that sensitive patient information will be purposefully tapped and hacked on an industrial scale from these messaging systems onto the Secondary Uses Services has not been appreciated.

260 The information will not be deleted from the messaging systems even when it has been confirmed that the clinical information sent with the patient referral has been safely received into the care of the intended recipient. The message information will remain stored on Connecting for Health’s intermediate computers indefinitely. There is no suggestion that the messaging system for electronic transfer of entire records, when the patient transfers from one GP to another, dubbed “GP2GP”, is any better protected.

The Health and Social Care Act 2001

270 Connecting for Health claim that this processing of information is lawful by virtue of Section 60 of the Health and Social Care Act 2001. Along with the subordinate NHS(Control of Patient Information) Regulations 2002, Section 60 allows the release of identifiable patient information without consent. The process has to be approved by the Secretary of State on the recommendation of a specifically appointed and independent Patient Information Advisory Group (PIAG). Unfortunately the independence of the Patient Information Advisory Group is eroded by several members being concurrent leading participants in the design of the national database. This is an irreconcilable conflict of interest.

280 The collection and use of data by the Secondary Uses Service was approved by PIAG on 13th June 2006²¹. There is no explicit reference to approval for the release of the information by the current data holders. It seems to be assumed that the current lawful data holders will be wholly passive in this process. The notion that there should be an active decision with regard to providing or with holding data is not addressed. Even so, the Patient Information Group were “unconvinced” in respect of key parts of the application and. there is an insistence on review of the approval in 12 months time.

The PIAG minute confirms that the data might be used for none health service uses provided that this is on a “statutory basis”. This confirms that third parties, (such as

²¹ Patient information Advisory Group Minutes 13/06/06 Para 7.1
<http://www.advisorybodies.doh.gov.uk/piag/2006%20June%20Minutes.pdf>

(The approval is not yet logged in the web based PIAG register of approved proposals and the submitted application is not on the site.)

290 the police, the Department for Work and Pensions, education and social services departments), may apply directly to the secondary uses database for information about named individuals that they would now be obliged to try and obtain via involved clinicians.

On the same statutory grounds it might be possible for the stored information to be searched for individuals whose records contain specific criteria so that such individuals can be identified. E.g. “produce a list of all the boys of a particular ethnicity who live in a specific locality and who have a given blood group.”

300 However, guidance for organisations applying for PIAG approval is clear²². PIAG powers cannot be used

- in circumstances when it is practicable to seek patient consent, and/or
- to over-ride the dissent of patients.

This plain English guidance derives from subsections 3 and 6 of section 60²³, where it is confirmed that the duties under the Data Protection Act are explicitly not over-ridden²⁴ and that the common law duty to obtain consent remains when ever it is “practicable”.

310 Clinicians regularly seek explicit consent. The notion that this is always “impractical” in respect of information released to the Department of Health, and yet, usually “practical” in respect of a myriad of other agencies is unsustainable.

320 Indeed, in the most recent draft minutes of the Patient Information Advisory Group²⁵ the secondary uses service is acknowledged to be unlawful. “A number of uses of data not covered, either by the class regulations or by the way section 60 has been framed, have been identified” Of concern, rather than make the data flow consent based and lawful, they continue: “It has been mooted therefore that consideration should be given to how either the class regulations or primary legislation might be reframed to encompass such uses.”

There is much in the 2001 legislation which renders patient information vulnerable. The legislation was strongly criticized by both the BMA and the RCGP during it’s progress through parliament. More recently a “consolidating” section was included in the NHS Act 2006²⁶. This may have endeavoured to erode these safeguards. But CfH’s claim that clinicians might over ride patient dissent to place information on the national database are contrary to the safeguards in the recent legislation. PIAG approval for the unconsented release of information by care workers is ultra vires.

²² <http://www.advisorybodies.doh.gov.uk/piag/applications.htm>

²³ <http://www.opsi.gov.uk/ACTS/acts2001/10015--g.htm#60>

²⁴ DPA requirements discussed more fully at <http://www.ardenhoe.demon.co.uk/privacy/NHS%20database%20proposals%20unlawful.pdf>

²⁵ Draft minutes Patient information advisory group meeting held Wednesday 13 December 2006 <http://www.advisorybodies.doh.gov.uk/piag/piag131206minutes.pdf>

²⁶ NHS Act 2006 section 251 & 252 <http://www.opsi.gov.uk/ACTS/acts2006/60041-af.htm#251>

330 In 2001 the Department of Health went to court to prevent the release of prescription information by chemists to pharmaceutical companies, even though the information was anonymised²⁷. There is a need to protect anonymised data. The Data Protection Act provisions do not apply to truly anonymised data. However, if health information is combined with associated, non-identifying data, such as age, NHS Trust or date of admission and discharge, it may be possible to deduce the identity of a patient, especially if the disease they suffer is rare. This is more likely to happen with the increased use of large databases that can be cross-referenced or by the use of powerful search engines. This was not the argument used by DoH in Source informatics²⁸.

340 The Department of Health was over ruled. But the legal argument showed that substantial quantities of sensitive patient information circulated within the NHS was unlawful because it was identifiable, unconsented and patients were unaware of its use.

The court's legal analysis replicated the findings of a Department of Health expert committee, the Caldicott committee. They had previously recommended that information flows should be made lawful. But rather than, ensure that information flows became anonymised or consented, the Department of Health changed the law.

350 **Lord Phillip Hunt**

Lord Warner's successor as Health Minister in the House of Lords is Lord Phillip Hunt. Having been a Health Minister previously, Lord Hunt has an important track record in respect of the confidentiality and privacy of patient's medical records. He knows all about these limited safeguards in this legislation because he was the Minister responsible for taking both Section 60 and the subordinate regulations through parliament in 2001 and 2002. It was Lord Hunt who introduced these safeguards to counter allegations from patient and professional bodies that the power's being sought by Government were authoritarian and excessive for the purposes claimed. Lord Hunt will recall the assurances that he gave to parliament in the various intelligent debates.

*"With the best of intentions, the NHS has had a tradition for paternalism where much of what is done in the name of science or research relies on the implied consent of patients, but that implied consent has been pushed too far. We saw that example at Alder Hey. There the issue was human organ retention. We see it in many places where confidential patient information is currently used. The most important lesson to be learnt from Alder Hey is that patients' trust will be lost if we fail to forge new relationships based on informed consent."*²⁹

370 **Risk analysis**

Connecting for Health's own clinical risk analysis³⁰ concluded that patient care would probably be safer using locally held sealed envelopes rather than storing them on the

²⁷ <http://www.hmcourts-service.gov.uk/judgmentsfiles/j4/source.htm>

²⁸ <http://www.parliament.uk/documents/upload/POSTpn235.pdf>

²⁹ Lord's Hansard 3 May 2001 column 865
<http://www.publications.parliament.uk/pa/ld200001/ldhansrd/vo010503/text/10503-13.htm>

³⁰ Sealed Envelopes Risk Assessment Project: Report for NHS Connecting for Health Revision 2
<http://www.nhsconfidentiality.org/wp-content/uploads/November%20-%20NHS%20Care%20Records%20Report.pdf>

NHS data spine. They were clear that the proposals would inhibit patients from attending or from divulging information to clinicians.

Privacy v. Research: The mythical conflict.

380 It is now clear that Lord Warner's "opt out" is limited to the summary care record. The legal, ethical and political justifications apply robustly to further aspects of the national database proposals. IT developments within the NHS that are essential for patients, clinicians and researchers will fail unless these matters are addressed.

There is no conflict between respecting patient control over information in both clinical care and in medical research. For as long as information is shared routinely without respecting patient wishes, substantial important information will be withheld from all of us – to the detriment of both care and research.

390 It is better for researchers to have access to reliable information from most people than unreliable information from everybody.

There is no justification to downgrade BMA and RCGP policy that requires the patient to explicitly permit any recording of information on the national database. There is certainly no justification for a system of compulsory data recording with a limited "opt-out" from just one component of the database. This "concession" from the ministerial working party is not sufficient to meet the professional, ethical and legal obligations on health workers to whom confidential sensitive information is first entrusted.

Focus the objectives, change the implementation.

400 Clinical care has become increasingly multidisciplinary, multitechnology and multivenue such that there are increasing problems with the paper records not being available to clinicians and patients when they meet.

410 The need for IT systems in hospital that are at least as good as the established systems in General Practice is unarguable. It is wholly understandable that clinicians and the public should have rallied behind a commitment to NHS I.T. at the highest level. It is also understandable that some enthusiasts might remain loyal to the current proposals for fear that the ring fenced resources might otherwise be diverted away from NHS IT. But such fears should not be allowed to drive through proposals, which when scrutinized have been found to be flawed.

British Computer Society Report

The near simultaneous publication of a key report from the British Computer Society³¹ was overshadowed by Lord Warner's parting announcement. The BCS

³¹ The Way Forward for NHS Health Informatics; Where should NHS Connecting for Health (NHS CFH) go from here?
<http://www.bcs.org/server.php?show=ConWebDoc.8951>

report is an informed and considered indictment of CfH strategy to date. Their key recommendation is to put the Personal Spine Information Service “on the back burner”. In essence they recommend a move to local databases with good quality secure communication between them. They suggest systems which provide better privacy and confidentiality as well as providing better usability and care. The BCS recommendations are likely to provide better quality data for research and managerial purposes and merit wider critical discussion and debate.

Conclusion

The patient’s consent decision can be changed in either direction with time. The decision will be based on balanced information and eventually on experience. Glossy promotion and razzmatazz that fails to mention the privacy side effects of the IT “treatment” will not suffice. Patients must be informed that the “treatment” is not obligatory. **The National Care Records Guarantee must be amended.**

Clinicians are under an obligation to keep records of the care provided. CfH however have tried to assert that such a record must be recorded as a “detailed care record” on their database. It is doubtful that there are powers to oblige clinicians to place the records they make on the national database system. There is certainly no mandate to oblige clinicians to place those records on the database contrary to the expressed wishes of the patient.

As a worst case option clinicians can keep information on paper records. As a better option, properly functioning and genuinely secure local databases would be preferable to paper in respect of care and more acceptable than the CfH proposals to patients in respect of privacy.

Subsequent to the Guardian initiated letters to the DoH, an empowering directive has been provided by a substantial number of patients to their General Practitioners in a letter format suggested at www.thebigoptout.com .

These mandates require and empower the General Practitioner not to place the patient’s data (or that of their children) on the national database. The mandates enable the GP to record patients wishes on their computer systems using the “Read code 93C3”. The text of those letters can reasonably be taken to include Detailed Care Records on CfH controlled servers, “Choose and Book”, “Electronic Transfer of Prescriptions” and “Healthspace”. Information will otherwise be taken from all these sources and then stored and transmitted in identifiable form in the Secondary Users Service – which is also excluded by the patients’ mandate.

An opt out from only the “summary care record” is essential but not sufficient to satisfy the mandate which has already been sent by thousands of patients to their GP. Connecting for Health, through it’s Summary Care Record Advisory Group, cannot simply assume that the patient opt out mandate applies only to the summary care record.

The new Health Minister, Lord Hunt is under an obligation to ensure that the safeguards that he put in place when he introduced the legislation are now respected.

470 Dr Paul Thornton MPH, FRCGP
Pear Tree Surgery
28 Meadow Close
Kingsbury
B78 2NR

Email paulthornton@beeb.net

8 March 2007

This document is accessible on line at
<http://www.ardenhoe.demon.co.uk/privacy/decoy.pdf>

480