

EVERY SINGLE PATIENT SHOULD OPT OUT OF THE NHS DATABASE WITHOUT DELAY

The Labour government is desperately hoping to transfer everyone's medical records to yet another centrally-held, government-controlled database, making patients' medical records potentially viewable to anyone working within the NHS. Your GP records would ultimately be no longer held at the surgery and the Department of Health would become the data-controller for your medical records, replacing your GP.

In January 2008 a poll by the British Medical Association revealed that nine out of ten doctors have no confidence in the government's ability to safeguard patients' data online or felt that they were in a position to assure patients that their data would be safe.

The unbelievable data protection breaches that were realised towards the end of 2007, including the loss of 25 million child benefit records and 15,000 pension policy records by Revenue and Customs, personal financial details of 40,000 housing benefit claimants by the Department of Work and Pensions, personal details of 6,000 people and details of 3 million candidates for the driving theory test by the DVLA, and in 2008 the loss of unencrypted personal, medical and financial details of 600,000 applicants for the Armed Forces by the MoD as well the loss of four discs containing personal and confidential details of magistrates court cases by the Ministry of Justice simply illustrate the very real dangers of choosing to upload personal data to huge centralised government databases.

In April 2007, The Department of Health (DoH) made the personal details – including religious beliefs and sexual orientation – of medical students applying for their first posts as doctors available to view on a public and unsecured website. The Information Commissioner's Office declared the DoH in breach of the Data Protection Act over this appalling action.

In May 2007, the Foreign and Commonwealth Office (FCO) was responsible for personal data of people applying for visas to enter the UK being visible to others visiting the application website. The Information Commissioner's Office declared the FCO in breach of the Data Protection Act over this appalling action.

In January 2008 the Ministry of Defence (MoD) admitted to losing unencrypted personal, medical and financial details of 600,000 applicants for the Armed Forces.

Also in January 2008, the Ministry of Justice admitted that four computer discs containing personal and confidential details of magistrates court cases went missing in the post.

In February 2008 the Home Office admitted that it had lost, for more than a year, a computer disc containing details of 4,000 DNA profiles of suspected foreign criminals. The failure to correlate that lost data with our own has had serious implications for the public safety of UK citizens.

Official figures revealed through parliamentary answers show that in the last year all government departments reported at least 208 laptops, and a number of PCs, stolen – many holding sensitive (and probably unencrypted) information. Since 1997 nearly 1,600 government computers containing sensitive information have been stolen.

Multiple NHS trusts have also admitted to losing sensitive details of hundreds of thousands of patients, adults and children, as well as personal details of their own NHS staff. More than 4000 NHS computer "smartcards", used to give access to confidential patient records on the NHS Database, have been reported as lost or stolen.

There seems to be no end to the amount of personal, medical and financial data this Government is able to lose.

On the 3rd January 2008 the Justice Select Committee produced a damning report into the way that the Government mishandles private data in the wake of the HMRC child benefit records scandal. To quote the report:

- "The roll call of banks, retailers, Government departments, public bodies and other organisations which have admitted serious security lapses is frankly horrifying."
- "We are extremely concerned to hear from the Information Commissioner that there are more cases involving the loss of personal data which have not yet fully come to light. The warning which he issued in the summer about the dangers of mishandling personal data and the extensive security lapses in a wide range of organisations has been proved correct."
- "There are, however, substantial risks associated with large databases which contain personal data and which are open to large numbers of licensed users."
- "There is evidence of a widespread problem within Government relating to establishing systems for data protection and operating them adequately."

Many people believe that the Labour government will abuse such uploaded data, for example to sell to pharmaceutical firms, big business and insurance companies; and with good reason - the DVLA alone has sold 5.3 million driver records to private companies since 2002.

Your data will be available, without your consent and in an identifiable way, to thousands of non-clinical health administrators under what is known as “Secondary Use Services”.

There is every reason to believe that the Labour government intends linking the NHS Database to its other huge databases – such as the Child Records Database, the DVLA databases, Revenue & Customs databases and, most worryingly, the National Identity Register (ID Cards) and the DNA Database.

Many believe that these databases, including the NHS Database, represent fundamental attacks on our basic right to privacy. In the words of the Information Commissioner himself, the UK is "in danger of sleepwalking into a surveillance society". Britain has more CCTV cameras than any country in the world. We have the biggest DNA Database in the world. We have become one of the most bugged, surveyed and monitored countries on Earth.

The Labour government wants patient’s medical records to be uploaded by default, unless the patient actively objects – an “opt out” mechanism: that is, if you do and say nothing, your notes will be uploaded. The British Medical Association, as well as many GPs, believes that patient should be asked for their *explicit* consent prior to any information being uploaded, i.e. an “opt in” mechanism: your notes should remain with your GP *until such time as you indicate that you actively wish for them to be uploaded (if ever)*.

The Oaklands Practice will never upload your medical details to the NHS database without your active and explicit consent. Many GPs will not accept an “opt out” mechanism for such uploads. However, a desperate government might stop at nothing to achieve its political aims, and that includes coercing or forcing GPs to upload data. But they *cannot* upload data from patients who have “opted out”. I have opted out, as have many GPs and their families.

More than eight out of ten doctors in the BMA's poll said that they would not want their own personal information stored on the NHS Database.

You DO NOT need to make an appointment with a GP to opt out. Just list your names on our opt-out form and hand it to reception. You can email the opt out form to us as well (details on our web site).

You have a choice. You do not have to allow your medical records to be uploaded to the NHS Database.

You do not have to give reasons for opting out. You do not have to justify your right to privacy.

Opting out will IN NO WAY affect the medical care and treatment that you receive from the Oaklands Practice, or affect the ability for your GP to refer you to a specialist for further care, should this be necessary. You remain fully (and legally) entitled to all the NHS care that you require, either from a GP, hospital A&E department or a hospital specialist.

You have nothing to lose by opting out now. You can opt in to the NHS Database at any time in the future.

Please feel free to take away and give copies of this handout to your family, friends and neighbours. This handout, our opt-out form, and a generic opt-out form for use at any GP surgery, are all available to download from our web site (www.oaklands.info).

PLEASE - DO NOT PUT YOUR PERSONAL AND SENSITIVE MEDICAL DATA AT RISK.

How much do you trust this Government?

Dr Neil Bhatia
Caldicott Guardian for the Oaklands Practice

For detailed information regarding opting out, please visit the following web sites:

- www.nhscarerecords.nhs.uk
- www.nhsconfidentiality.org